Counter-Fraud Policy and Fraud Response Plan

Document Control	
Document Type:	Policy
Department:	Finance
Relevancy:	Group Wide
Owner:	Alison Close
Approver:	Audit & Risk Committee
Published Date:	22/09/2023
Version:	1
Security Classification:	Internal
Last Review Date:	01/03/2023
Next Review Date:	01/03/2026

LTE Group – Counter-Fraud Policy and Fraud Response Plan

Key Contact Details

All LTE Group colleagues and **members of the LTE Group Board** are expected to **promptly report** (in line with the guidance set out in the Fraud Response Plan) **all legitimate concerns** about suspected fraud or irregularity.

Position	Name	Contact Details
Chief Financial Officer	Alison Close	AClose@ltegroup.co.uk
Company Secretary & General Counsel	Lorna Lloyd-Williams	llloydwilliams@ltegroup.co.uk
CEO / Accounting Officer	John Thornhill	John.Thornhill@ltegroup.co.uk
Audit & Risk Committee Chair	Philip Lanigan	To be contacted via the Governance team.

You can also contact **Action Fraud** on 0300 123 2040 or report it online www.actionfraud.police.uk.

Measures of Protection
The LTE Group Public Interest Disclosure Policy provides details of the measure of protection that may be allowed to individuals in making disclosures of potential irregularities, including fraud, corruption or impropriety.

Contents	Page

Purposes of Policy and Fraud Response Plan

The purpose of this policy is to:

- communicate LTE Group's zero-tolerance stance on fraud;
- make all colleagues and the Board of Governors aware of the risks of fraud, and what their responsibilities are regarding safeguarding the proper use of LTE Group's finances and resources against fraudulent or corrupt acts;
- foster a culture that deters fraudulent or corrupt activity, encourages its preventions and promotes its detection and reporting; and to
- help reduce instances of fraud perpetrated against LTE Group to the absolute practical minimum.

The purpose of the Fraud Response Plan is to:

- provide guidance to colleagues in the event that they suspect that a fraud or irregular activity is, or has been, taking place;
- provide a framework response plan for investigating and reporting all suspected frauds, with clearly defined roles, responsibilities and timescales;
- to ensure that in the event of fraud, timely and effective action is taken to prevent further losses, and to
- ensure that if a fraud is proved, the necessary sanctions are imposed.

Policy Scope

This policy applies to all colleagues and associated persons of LTE Group (both internal and external to the organisation).

Where applicable this includes:

- Members of the LTE Group Board
- All Employees (including those employed by subsidiary companies)
- Agency Colleagues
- Contractors (including MOL Associates)
- Consultants
- Suppliers
- Service Users (including learners, students, apprentices, working professionals and offenders)
- Employees and committee members of organisations funded by the organisation
- Employees and principals of partner organisations

This policy is operated in conjunction with the **Financial Regulations** and other related LTE Group policies, including the **Public Interest Disclosure and Whistleblowing Policy**, the **Anti-Bribery and Corruption Policy** and the **Anti-Money Laundering policy**.

Statement of Commitment to Ethical Behaviour

LTE Group has a **zero-tolerance stance on fraud**, and requires all colleagues, students, Board members and any other associated persons to act, at all times, honestly and with integrity.

LTE Group recognises that it derives a significant amount of its income from public resources, and has a duty to ensure value for money is secured from public funds. The Group is committed to protecting its operations and reputation and its funders, colleagues, students and Board members from the detriment associated with fraud and other corrupt activity.

LTE Group recognises that robust anti-fraud culture underpins all actions taken to prevent fraud. The Group is committed to promoting an organisational culture that encourages the prevention of fraud and corruption, by raising awareness of all colleagues of the need for high standards of personal conduct.

LTE Group is committed to conducting its activities fairly, honestly and openly, in accordance with relevant legislation, and to the highest standards of integrity. The Group is committed to the following three fundamental public service values, which are:

- **Accountability**: Everything done by those who work in the organisation must be able to stand the test of parliamentary scrutiny, public judgements on propriety and professional code of conduct.

- **Probity**: Absolute honesty and integrity should be exercised in dealing with students, assets, colleagues, suppliers and customers.

- **Openness**: The organisation's activities should be sufficiently public and transparent to promote confidence between the college and its students, colleagues and the public.

All colleagues, and associated persons of LTE Group, are accountable and responsible for upholding these values, and for reporting any action to the contrary.

Please also see **Appendix 1**, for the **Code of Conduct** which all colleagues are required to follow when undertaking their duties.

Fraud: Definitions and Examples

The Fraud Act 2006 came into force on 15 January 2007. Full details of the Act are available at: http://www.legislation.gov.uk/ukpga/2006/35/contents.

The Act defines the legal definition of fraud as:

'The making of a false representation or failing to disclose relevant information, or the abuse of position, in order to make a financial gain or misappropriate assets'.

The Act lists three main offences, which are:

- **Fraud by false representation** - A representation is false if it is untrue or misleading and results in a financial gain for themselves or anyone else, or inflicts a loss (or a risk of loss) on another.

- **Fraud by failing to disclose information** – A person is in breach of this section if they fail to disclose to another person information which they are under a legal duty to disclose and results in a financial gain for themselves or anyone else, or inflicts a loss (or a risk of loss) on another.

- **Fraud by abuse of position** - A person is in breach of this section if they abuse their position of authority or trust within the organisation for a personal or financial gain or inflicts a loss (or a risk of loss) on another.

The term 'fraud' is usually employed to describe acts such as theft, embezzlement, misappropriation, bribery, money laundering, corruption, forgery, extortion, conspiracy, collusion, false accounting, false representation and concealment of material facts.

Significant fraud is usually where one or more of the following factors are involved:

- the sums of money are in excess of £10,000
- there is likely to be public interest because of the nature of the fraud or the people involved
- the particulars of the fraud are novel or complex
- the fraud is systematic or unusual in nature

At a practical level, fraud is deemed to be the deliberate attempt to deprive LTE Group (and its associate activities) of funds or assets. However, fraud can also be perpetrated against colleagues, students, suppliers, Government Agencies or Departments or the public. Fraud, by its inherent nature of deception to result in financial or personal gain, means that the transaction must be irregular and improper.

Examples - Please see **Appendix 2** for some **common examples of fraud**.

Proven Fraud or Attempted Fraud – Sanctions

To act as a deterrent to others, a main objective in any fraud investigation will be the punishment of the perpetrators.

Attempted fraud is treated as seriously, and bears the same consequences, as accomplished fraud.

LTE Group will instigate disciplinary procedures against any colleague or student who is proven to have committed fraud. LTE Group will normally involve the police, and pursue the prosecution of any such individual.

Where any proven fraud is committed against LTE Group, consideration will always be given to prosecuting the person/organisation responsible through all criminal and/or civil means available.

Statement of Responsibility – LTE Group

LTE Group are responsible for ensuring that expenditure and income are applied for the purposes intended by Parliament and that the financial transactions conform to the authorities that govern them. In addition, they are responsible for ensuring that funds from the Education and Skills Funding Agency (ESFA) are used only in accordance with the Financial Memorandum with the ESFA and any other conditions that may be prescribed from time to time.

LTE Group must therefore take all reasonable steps to prevent fraud from occurring. The Group must establish and maintain an adequate system of internal control, to ensure compliance, and to prevent and detect irregularities and suspected fraud (including theft, bribery and corruption).

The **LTE Group Board** is ultimately responsible for LTE Group's system of internal control and for reviewing its effectiveness. However, such a system is designed to manage rather than eliminate the risk of failure to achieve business objectives, and can provide only reasonable and not absolute assurance against material misstatement or loss.

The Group Board has delegated the day-to-day responsibility to the **Chief Executive Officer (CEO), as Accounting Officer**. The CEO is responsible for maintaining a sound system of internal control that supports the achievement of LTE Group's policies, aims and objectives, whilst safeguarding the public funds and assets for which he is personally responsible, in accordance with the responsibilities assigned to him in the Financial Memorandum between LTE Group and the ESFA. He is also responsible for reporting to the Group Board any material weaknesses or breakdowns in internal control.

Statement of responsibility – Audit and Risk Committee

As per the **Post-16 Audit Code of Practice**, the Audit and Risk Committee are responsible for:

- performing an annual review of the fraud register (see page 17);
- overseeing the corporation's policies on and processes around fraud, irregularity, impropriety and whistleblowing; and ensure:
    - the proper, proportionate and independent investigation of all allegations and instances of fraud and irregularity;
    - that investigation outcomes are reported to the Audit and Risk Committee;
    - that the external auditor (and internal auditor if applicable) are informed of investigation outcomes and other matters of fraud, irregularity and impropriety, and that appropriate follow-up action has been planned/actioned;
    - that all significant cases of fraud or suspected fraud, theft, bribery, corruption, irregularity, major weakness or breakdown in the accounting or other control framework are reported to ESFA as soon as possible; and that
    - risks around fraud have been identified and controls put in place to mitigate them.

Statement of Responsibility – Line Managers

LTE Group Line Managers are responsible for:

- implementing this policy in respect of fraud prevention and detection;
- identifying, and assessing the scale, of common types of fraud risk in their area and for briefing their team about these risks;
- implementing and documenting effective systems of internal control for managing and mitigating these risks, and for allocating responsibility for the operating of these controls;
- ensuring that these controls are constantly applied and that procedures are being followed, through routine checks and monitoring;
- identifying and investigating any areas in which controls are not being uniformly applied, and taking remedial action if required;
- performing thorough checks when authorising transactions such as expense claims, timesheets and purchase orders;
- setting a good example – line managers should comply, and be seen to comply, with all controls;
- taking prompt and appropriate action if a member of their team raises any concerns about suspected fraudulent activity; and
- providing support, as and when required, to fraud investigations.

The Chief Financial Officer and Internal Audit are able to offer advice and assistance regarding the implementation and documentation of effective systems of internal control.

Please also see **Appendix 3**, which provides guidance in the event of a suspected fraud of **Line Manager 'Dos and Don'ts'**.

Statement of responsibility – All Colleagues

All LTE Group colleagues are responsible for:

- complying with this policy, and ensuring that their interests, activities and behaviours do not conflict with these obligations;
- remaining alert and vigilant to the risk of fraud;
- protecting the assets and reputation of LTE Group;
- applying the internal controls, and rules and regulations that are designed to deter, prevent and detect fraud;

- completing and keeping up-to-date with all mandatory online training on fraud and cybercrime; and,

- promptly reporting (in line with the guidance set out in the Fraud Response Plan) all legitimate concerns about suspected fraud or irregularity.

Please also see **Appendix 4**, which provides guidance in the event of a suspected fraud of **Colleagues 'Dos and Don'ts'**.

Statement of Responsibility – External Organisations

All external organisations who deal with LTE Group, must:

- operate within the law and any specific agreements or contracts, and

- conduct themselves in accordance with usual ethical business standards, consistent with LTE Group's charitable status and public funding.

Statement of Responsibility – Internal Auditor

The Internal Auditor is **not** responsible for detecting fraud; this is the responsibility of LTE Group management.

However, the Internal Auditor can assist, by examining and evaluating the adequacy and effectiveness of LTE Group management's action to prevent, detect and investigate irregularities, including fraud and corruption.

For example, the Internal Auditor can:

- regularly review fraud policies, procedures, prevention controls and detection processes making recommendations to improve these processes as required;

- discuss with management any areas which it suspects may be exposed to fraud risk;

- help determine the appropriate response to a suspected fraud and to support any investigation taking place; and

- facilitate corporate learning on fraud, fraud prevention and the indicators of fraud.

The work of the Internal Auditor should be planned to take into account consideration of fraud, theft, corruption and risk assessment, especially in those systems where there is a significant risk of fraud. Systems should be tested to ensure that the risk of fraud, both internal and external, is minimised, and the Internal Auditor should be alert to any control weaknesses that allow fraud to occur.

Statement of Responsibility – External Auditor

The External Auditor is **not** responsible for detecting fraud; this is the responsibility of LTE Group management.

However, an auditor conducting an audit in accordance with ISAs (UK and Ireland) is responsible for obtaining reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error.

When obtaining reasonable assurance, the auditor is responsible for maintaining professional scepticism throughout the audit, considering the potential for management override of controls and recognising the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud.

Fraud and Cybercrime – Online Training

In response to the ever increasing threat of cybercrime, LTE Group has introduced mandatory online training to ensure colleagues are kept up-to-date with the risks that the Group faces and how to mitigate these risks.

This training is delivered through weekly, short online security courses, via the usecure security education system. Courses include (but are not limited to):

- Malware & Ransomware
- Social Engineering
- Using Social Media Safely
- Removable Media
- 7 Steps to Being Secure at Home

Appendix 1 – Code of Conduct

All those who work for, or are in contract with, the LTE Group should exercise the following when undertaking their duties:

● **Selflessness** - Should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family or their friends.

● **Integrity** - Should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.

● **Objectivity** - Should, in carrying out public business, (including making public appointments, awarding contracts, or recommending individuals for rewards and benefits), make choices on merit.

● **Accountability** - Are accountable for their decisions and actions to the public and must submit them to whatever scrutiny is appropriate to their office.

● **Openness** - Should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest demands.

● **Honesty** - Have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

● **Leadership** - Should promote and support these principles by leadership and example.

Appendix 2 – Examples of Fraud

Fraud could be committed by either people within LTE Group, or by external people.

Examples of fraud could include:

Procurement and Purchasing

- Conflicts of interest with third parties and acquaintances
- Offers of bribes/inducements
- Bid rigging
- Payoffs and kickbacks
- Colluding with suppliers to accept inferior goods or services
- Diverting goods or services for personal use
- Falsely creating or diverting payments
- Submission of false invoices
- Demands for payment of unsolicited goods

Banking

- Unauthorised access of bank accounts
- Attempting to change bank account details of suppliers and payees
- Identity theft where colleagues are persuaded to reveal login and passwords details
- Fraudsters impersonating senior colleagues to demand that a bank transfer is made to an improper account

Financial Records

- Under recording income
- Embezzlement
- Internal theft
- Falsifying accounting or other records
- Falsifying financial returns or claims
- Unauthorised removal or destruction of records
- Forgery or alteration of documents
- Use of the LTE Group name, logo or letterhead for personal reasons

Theft and Misuse of Information

- Unauthorised removal of LTE Group property
- Theft of LTE Group property
- Passing on company data or intellectual property
- Unauthorised disclosure of confidential information

iTrent

- Setting up dummy or ghost employees
- Unauthorised changes to iTrent
- Deliberately inputting incorrect details in e.g. additional hours worked
- Providing false self-certifications / medical fit notes

Fraudulent Claims

- Falsifying or manipulating receipts
- False / duplicate expense claims

Recruitment

- Fraudulent Curriculum Vitae (CV)
- Misrepresenting qualifications / certificates
- Falsifying documents such as passports and visas or other identification
- Fraudulent references
- Employing family or friends over better candidates

Teaching

- Falsifying examination results and awards

This list is illustrative and not exhaustive; other examples of fraud also exist.

Appendix 3 – Line Managers – Dos and Don'ts

DO

- **Do** be responsive to colleagues concerns, and treat all colleagues concerns seriously and sensitively.

- **Do** deal with the matter promptly, as any delay could cause LTE Group to experience financial losses and/or reputational damage.

- **Do** maintain confidentiality, and follow the escalation guidance set out in the **Fraud Response Plan.**

- **Do** record carefully all relevant details, and obtain as much information as possible from the reporting colleague. This should include a note of any documentary evidence that may support the allegations made.

- **Do**, if possible, take steps to minimise any immediate future losses.

DON'T

- **Don't** be afraid to seek advice from the appropriate person – as per the guidance set out in the **Fraud Response Plan.**

- **Don't** approach or accuse the individual(s) about whom the allegation has been made.

- **Don't** try to investigate the matter yourself, as there are special rules surrounding the gathering of evidence for use in criminal cases.

Appendix 4 – All Colleagues – Dos and Don'ts

DO

- **Do** report your suspicions promptly, either to your line manager or other responsible persons – as per the guidance set out in the **Fraud Response Plan.** Any delay could cause LTE Group to experience financial losses and/or reputational damage.

- **Do** make an immediate note of your concerns – i.e. all relevant details, such as the date, time and name of any parties involved, and details of the conversation.

- **Do** try to safeguard evidence, as a fraudster may try to destroy at the first opportunity. If necessary, try to discreetly copy documents (including electronic records).

- **Do**, where possible, try to preserve confidentiality. Only discuss with your line manager or other responsible persons.

- **Do** escalate to the Chief Financial Officer, if, after you have reported the incident, you are not, soon after, then contacted by the nominated fraud investigator(s).

- **Do** persist in raising your concerns, even if you are deterred from doing so.

DON'T

- **Don't** be afraid of raising any legitimate concerns. LTE Group will treat any matter you raise sensitively and confidentially. The LTE Group Public Interest Disclosure and Whistleblowing Policy outlines the measure of protection that may be allowed to individuals in making disclosures of potential irregularities, including fraud, corruption or impropriety.

- **Don't** confront an individual that you suspect is committing fraud with accusations of wrongdoing. This may result in the destruction of evidence, and, in extreme cases, might expose you to physical danger.

- **Don't** try to investigate the matter yourself, as there are special rules surrounding the gathering of evidence for use in criminal cases.

- **Don't** tell anyone else about your concerns, other than those with the proper authority.

- **Don't** allow your actions to be influenced by personal likes or dislikes. LTE Group will instigate disciplinary procedures against any colleague or student who makes a false or malicious allegation against another member of LTE Group.

Appendix 5 – Fraud Response Plan

Introduction

The Fraud Response Plan sets out LTE Group's procedures for ensuring that all allegations and reports of fraud or irregularity are properly and fairly investigated, and that prompt and effective action is taken.

Duty to report any suspicions of fraud or irregularity

All LTE Group colleagues and members of the LTE Group Board are responsible for remaining alert and vigilant to the risk of fraud, and for protecting the assets and reputation of LTE Group.

All LTE Group colleagues and members of the LTE Group Board have a duty to **promptly** report all legitimate concerns about suspected fraud or irregularity. All reports will be treated sensitively and in absolute confidence.

The LTE Group Public Interest Disclosure and Whistleblowing Policy outlines the measure of protection that may be allowed to individuals in making disclosures of potential irregularities, including fraud, corruption or impropriety.

Reporting route – option 1
Colleagues should immediately report their concerns to the **Chief Financial Officer**.

Reporting route – option 2
If colleagues would prefer, they can instead report their concerns to their line manager. However, if they are not then contacted shortly after by the nominated fraud investigator(s), they should escalate their concerns to the Chief Financial Officer.

Reporting route – option 3
If the matter to be reported concerns the **Chief Financial Officer**, or if he/she is unavailable, it should be reported directly to the **Company Secretary & General Counsel**.

Reporting route – option 4
If the matter to be reported concerns the **Company Secretary & General Counsel**, it should be reported directly to the **Chief Executive Officer**.

Reporting route – option 5
If the matter to be reported concerns the **Chief Executive Officer**, it should be reported directly to the **Chair of the Audit and Risk Committee**.

Please also see **Appendices 3 and 4**, which provides guidance in the event of a suspected fraud of both **Line Manager** and **Colleagues 'Dos and Don'ts'**.

Receipt of an allegation of Fraud

Within 24 hours of the incident being reported, the Chief Financial Officer should ensure all the details of the suspected fraud or irregularity have been recorded and verified with the individual who has made the report.

The Chief Financial Officer should then immediately share these details with the Company Secretary & General Counsel, and meet with him/her to discuss the most appropriate response.

Depending on the nature of the incident, the Company Secretary & General Counsel may also wish to invite all, or some, of the following to the meeting:

- the Chief Executive Officer (or nominee)
- the Deputy Chief Executive Officer (or nominee)
- the Chief Operating Officer (or nominee)
- the Group HR Director (or nominee)
- the Group IT Director (or nominee)
- a member of the Group's Internal Auditor's team

The purpose of this initial meeting is for the Company Secretary & General Counsel to appoint an appropriate investigating officer. It is important that the preliminary investigation is undertaken by an individual with the relevant experience. This may be a member of the Group's Internal Auditor's team, supported as necessary by LTE Group colleagues.

All alleged frauds should be investigated. Although an incident may, at first, appear to be only a minor fraud, this may conceal a much larger scale of losses.

At this initial meeting, the attendees should also consider whether any steps can be taken at this initial stage to prevent further losses, e.g. by suspending payments, or by removing an individual's system access. However, action should only be taken if it can be reasonably certain that this action will not alert the fraudster or compromise the quality of evidence.

Depending on the nature and severity of the incident, the Company Secretary & General Counsel should consider whether, ahead of the preliminary investigations, the suspected fraud should be reported to the Police, and/or other external parties, such as the ESFA.

Confidentiality

During the preliminary investigations, all reasonable steps will be taken not to breach confidentiality or to reveal the identity of the complainant.

If a formal investigation is later instigated, confidentiality will be maintained in so far as it is consistent with a fair investigation, and with the right of the person (or persons) being investigated to be aware of the nature of the concerns raised.

Preliminary investigations

Once appointed, the investigating officer should urgently undertake a review to establish whether or not there are prima facie grounds for the concerns about suspected fraud or irregularity.
The purpose of these preliminary investigations is to gather all relevant information and documentation to enable the Company Secretary & General Counsel to conclude whether or not there is a case for further investigation / action.

During the preliminary investigations, the investigating officer is responsible for providing regular and confidential updates to the Chief Financial Officer and the Company Secretary & General Counsel.

Upon completion of the preliminary investigations, the investigating officer should formally report to the Company Secretary & General Counsel whether or not grounds for concern are shown to exist.

Outcome - no grounds for concern

If the preliminary investigations show no grounds for concern, then the matter may be dismissed.

The investigating officer is responsible for communicating this decision to the individual who reported the suspected fraud or irregularity.

The individual may, within 14 days of receipt of this notification, submit a written request to the Chair of the Audit and Risk Committee (if the issue falls within the purview of that Committee) or the Chair of the Board of the LTE Group that the decision be reviewed. This request should explain why they are dissatisfied with the outcome of the investigation of their concern. The Chair of the Audit and Risk Committee/Chair of the Board will consider the information considered by the investigation, the procedures that were followed and the reasons for not taking any further action. The outcome of this will be either to confirm that no further action is required or to decide that further investigation is required.

Outcome - grounds for concern

If the preliminary investigations show there are grounds for concern, then a formal investigation will be launched.

Again, depending on the nature and severity of the incident, the Company Secretary & General Counsel should consider whether, ahead of the formal investigation, the suspected fraud should be reported to the Police, and/or other external parties, such as the ESFA.

If there is a delay in contacting the Police, this may prejudice further enquiries. In addition, if the Police are alerted immediately, they may be able to offer advice on how best to proceed and on the most effective methods of evidence gathering.

Prevention of Further Loss

If the preliminary investigations show there are grounds for concern, then the Company Secretary & General Counsel should, in conjunction with relevant colleagues, decide how to prevent further loss.

This may require the suspension, with or without pay, of those under suspicion. However, it may be necessary to plan the timing of this suspension, to prevent the removal and/or destruction of evidence. This evidence may be required to support any subsequent disciplinary or criminal action. If the decision is made to remove those under suspicion from LTE Group's premises, the personal safety of colleagues should be considered. The suspect(s) should be approached unannounced, and by at least two people. Please refer to LTE Group Disciplinary policy when considering suspension.

Before leaving LTE Group's premises, the suspect(s) should be supervised at all times. They should be allowed, under supervision, to collect any personal property. However, they should not be allowed to remove any LTE Group owned property (including mobile devices). Any security passes and keys to premises, offices and furniture must be returned.

In addition, the suspect(s) access permissions to all LTE Group's systems must be removed immediately.

Formal investigation

Under normal circumstances, the investigating officer who performed the initial review, shall be requested to lead the formal investigation. However, if it is deemed more appropriate, the Company Secretary & General Counsel may consider appointing an external person to lead this work, e.g. a forensic accountant.

In some instances, the investigating officer may discover during the investigation that technical expertise is required that they do not possess. The Company Secretary & General Counsel should then re-assess whether or not they need to appoint external specialists to lead or contribute to any further investigations.

Prior to the investigation, the Company Secretary & General Counsel should agree the following:

- a detailed remit and scope for the investigation
- reporting procedures and deadlines
- a programme of regular meetings

During the investigation:

- The investigating officer and their team will have full access to all LTE Group colleagues, and will be entitled to their full co-operation. Any failure by colleagues to co-operate fully with an investigation, may, in itself, constitute grounds for disciplinary action.

- The investigating officer and their team will also have full access to all required buildings, systems and records (both manual and electronic). However, they will aim to minimise disruption to operational activities and processes.

- The investigating officer should record all details fully, accurately and in a manner that is accessible.

It is essential that any action, or gathering of evidence, does not prejudice LTE Group's ability to prevent fraudulent activity or to recover losses incurred through fraud.

Formal investigation report

Upon the completion of the formal investigation, the investigating officer should produce a draft formal investigation report. This report should then be agreed by the Chief Financial Officer and the Company Secretary & General Counsel, who if necessary, should consult with the Chief Executive Officer. The report may then be finalised.

This report shall contain:

- a description of the suspected fraud or irregularity
- the people involved and the means by which the fraud was allowed to occur (if applicable) - highlighting any control and/or operating weaknesses within the systems
- all possible facts ascertained relating to the alleged fraud
- a conclusion as to whether the allegations made had any substances
- the value and extent of any loss or adverse impact to LTE Group

If the allegations are deemed to have substance, the report shall also contain:

- details of any regulations, policies or procedures that were breached
- the steps taken to mitigate any losses to LTE Group
- the actions taken to-date regarding the individual(s) concerned and any recommendations regarding future actions
- a review of the timeliness and effectiveness of responses
- details of any lessons learned during the investigation
- the measures recommended to minimise the risk of a recurrence
- any other relevant material

This report should be presented both to the Chief Executive Officer, and to the Audit and Risk Committee.

Recovery of losses

A key objective of any fraud investigation should be to recover losses. The investigating officer should ensure that, in all fraud investigations, the amount of any loss will be quantified. In all cases, repayment of losses should be sought.

Where the loss is substantial, legal advice should be taken about the need to freeze the suspect's assets through court, pending conclusion of the investigation. Where the perpetrator refuses payment, legal advice should also be taken about the prospects for recovering losses through the civil court. LTE Group would normally expect to recover costs in addition to losses.

LTE Group's insurers should be made aware of the pursuit of any such claims.

Outcome – no fraud proven

If, on the basis of the evidence, no fraud is proven, then the Chief Financial Officer is responsible for informing all relevant parties. The suspension must be lifted immediately and the line manager will contact the colleague to facilitate a return to work.

Outcome – fraud proven

If, on the basis of the evidence, a fraud is proven, then, as Accounting Officer, the Chief Executive Officer is responsible for:

- ensuring that action is taken in line with LTE Group's formal disciplinary procedures;
- ensuring that the incident is reported, where necessary, to external bodies such as the Police (if not previously reported during the course of the investigation), the ESFA and the Office for Students (OfS); and
- ensuring that civil action is taken to recover any losses.

Other reporting requirements

- As per the ESFA's post-16 audit code of practice, in the event that a fraud, theft, bribery, corruption, irregularity, major weakness or breakdown in the accounting or other control framework is identified, LTE Group must inform the Chair of the Audit and Risk Committee, the External Auditor and the Internal Auditor as soon as practically possible.
- **ESFA** must also be informed when the amounts are significant, that is **exceeding £10,000** in value, as soon as possible.
- As per the **Office for Students, (OfS)** terms and conditions of funding for higher education institutions, they should be informed of all significant frauds, which is defined as those **exceeding £25,000**.
- Depending on the nature of the fraud, other external bodies may need to be informed, e.g. HM Revenues and Customs.
- Significant fraud, including any suspected or attempted fraud, should be reported to **Action Fraud** to help identify systematic risks potentially affecting whole sectors (for example cybercrime). Action Fraud monitors the cost of fraud across the UK and has been set up to provide a single point of reporting and information for individuals and organisations.
- The additional requirement to report fraud as a breach of regularity does not alter, reduce or replace the standard reporting requirements for fraud including the Proceeds of Crime Act 2002.

Fraud register

The Chief Financial Officer is responsible for maintaining a fraud register. For every suspected fraud or irregularity report, details will be recorded on the register of:

- the date the incident was reported
- a description of the incident
- whether or not a fraud or irregularity was proven
- the outcome of any investigation
- the cost and/or adverse impact on LTE Group
- details of any Police involvement
- date reported to the Audit and Risk Committee
- details of any communications to external authorities
- actions taken to improve the control environment