Anti-Money Laundering Policy

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:	01/07/2023
Next Review Date:	01/03/2026

LTE Group – Anti-Money Laundering Policy

All LTE Group colleagues and **members of the LTE Group Board** are expected to **immediately report** (in line with the guidance set out below) **all legitimate concerns** about suspected money laundering activity.

Failure to do so could result in the colleague or Board member becoming personally liable to prosecution.

Position	Name	Contact Details
Company Secretary & General Counsel / **Money Laundering Reporting Officer (MLRO)**	Lorna Lloyd-Williams	llloydwilliams@ltegroup.co.uk
Chief Financial Officer / Money Laundering **Compliance Officer (MLCO)**	Alison Close	AClose@ltegroup.co.uk
CEO / Accounting Officer	John Thornhill	llloydwilliams@ltegroup.co.uk
Audit & Risk Committee Chair	Philip Lanigan	PLanigan-Gov@ltegroup.co.uk

While it is hoped this policy will reassure colleagues to raise concerns internally, you can also contact **Protect** (formerly Public Concern at Work) for independent and confidential advice on:

Telephone: 020 3117 2520
Email: whistle@protectadvice.org.uk
Website: whistle@protectadvice.org.uk

Reporting route – option 1
Colleagues should immediately report their concerns to the Company Secretary & General Counsel, who is the Group's **Money Laundering Reporting Officer (MLRO)**.

Reporting route – option 2
If the matter to be reported concerns the **Company Secretary & General Counsel**, or if he/she is unavailable, it should be reported directly to the Chief Financial Officer, who is the **Group's Money Laundering Compliance Officer (MLCO)**.

Reporting route – option 3
If the matter to be reported concerns the **Chief Financial Officer**, it should be reported directly to the **Chief Executive Officer**.

Reporting route – option 4
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**.

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.

Purposes of Anti-Money Laundering Policy

This policy has been introduced in response to UK Legislation enacted to combat money laundering.

The purpose of this policy is to:

- communicate LTE Group's zero-tolerance stance on money laundering;
- make all colleagues and the Board of Governors aware of the risks of money laundering, and what their responsibilities are with regard to observing and upholding the Group's position;
- provide guidance to colleagues in the event that they suspect that money laundering is, or has been, taking place;
- foster a culture that deters money laundering, encourages its preventions and promotes its detection and reporting; and to,
- ensure that in the event of suspected money laundering, timely and effective action is taken, and, in the event that a colleague is involved in criminal activity, that sanctions are imposed.

Policy Scope

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

Where applicable this includes (but is not limited to):

- 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

Third parties will be bound by any contractual obligations relating to anti-money laundering, as set out in contracts and agreements.

This policy is operated in conjunction with the **Financial Regulations** and other related LTE Group policies and procedures, including the **Public Interest Disclosure and Whistleblowing Policy**, the **Counter-Fraud Policy and Fraud Response Plan**, the **Anti-Bribery and Corruption policy** and the **Gift and Hospitality Policy**.

Statement of Commitment to Ethical Behaviour

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

In accordance with Managing Public Money (MPM) the Group is committed to the highest level of openness, integrity and accountability, both in letter and in spirit, and is committed to being compliant with all relevant legal and regulatory obligations. This includes adherence to the UK legislation enacted to combat money laundering and to the prevention of criminals from being able to use the Group to help them launder money, or to finance terrorism.

The Group is committed to protecting its operations and reputation and its funders, colleagues, students and Board members from the detriment associated with money laundering and other corrupt activity, and is, therefore, committed to:

- complying fully with relevant UK legislation in relation to anti-money laundering;
- ensuring that it has a sufficient risk-based and proportionate approach to due diligence concerning the Group's anti money laundering responsibilities;
- ensuring sufficient safeguards and an internal control system are in place throughout the organisation to minimise the risk of the Group and its colleagues from being exposed to money laundering;
- training colleagues on how to spot potential signs of money laundering activity;
- providing colleagues, and associated persons of LTE Group, with a clear reporting structure for any instances in which it is suspected money-laundering is taking place;
- the rigorous investigation of any such allegations; and to,
- taking appropriate action in instances where money-laundering is found to be taking place, including any required external reporting.

The Group is committed to tackling malpractice. We will act ethically and with integrity in all our relationships and will use all reasonable endeavours to take action against malpractice, wherever we can do so.

For the avoidance of doubt, the Group will not do business with anyone whom it is suspects of taking part in any activity, knowingly or unknowingly, which it regards as linked with potential money-laundering.

Money Laundering: Definition

The Proceeds of Crime Act 2002 (POCA) defines money laundering as:

'*The process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently or recycled into further criminal enterprises.'*

The process of money laundering takes criminally-derived 'dirty funds' and converts them into other assets or funds. This conceals the true origin or ownership of the funds, and so 'cleans' them, because the clean money or assets do not have an obvious link with any criminal activity.

Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.

Financial transactions that carry a higher risk of money laundering are those where there are large volumes of cash transactions and those where customer identification is more difficult, for example if the customer is based overseas.

There are three stages in money laundering:

- **Placement** – where the proceeds of criminal laundering enter into the financial system;

- **Layering** – distancing the money from its illegal source through layers of financial transactions; and,

- **Integration** – reintroduction of illegal proceeds into legitimate commerce by providing an apparently genuine explanation for the funds.

Within the education sector, one example of money laundering could be if a criminal used 'dirty funds' to make a cash payment of student fees (**placement**), but then followed this with a request to make an electronic refund to a bank account (**layering**). If the education establishment did not have adequate money laundering controls in place and made the refund, then the criminal would then have a bank statement showing a refund from the education establishment. If the criminal was then investigate they would be able to then give an apparently genuine explanation for the funds (**integration**).

The 2020 'National risk assessment of money laundering and terrorist financing' cites an example of money laundering in the education sector, by reference to a 2017 Guardian article about the money laundering scheme known as the 'Azerbaijani Laundromat'.

The report states that '…*funds are reported to have passed through several companies before being used to pay fees for private education in the UK. Due to this laundering method, the school in question would not have immediately known that there was any cause for concern around the ultimate source of these funds*.'

Money Laundering: Legal Framework

In the UK, the approach to money laundering and terrorist financing is based on objectives that are specified in legislation and/or Financial Conduct Authority rules.

The UK Anti-Money Laundering Legislation framework is complex and continually evolving. Key elements include:

Primary legislation consists of:

- Proceeds of Crime Act 2002 (as amended)
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
- Counter-terrorism Act 2008, Schedule

Secondary legislation is the Money Laundering Regulations (MLRs) which supports the primary legislative objectives:

- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- the Money Laundering and Terrorist Financing (Amendment) Regulations 2019
- the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020

The **Money Laundering Regulations 2017 (MLR 2017)** transpose the EU MLDs into domestic law and sets out basic requirements for 'regulated businesses' to help identify suspected corrupt wealth, including:

- know your customer (KYC) screening (such as obtaining beneficial ownership information and undertaking due diligence checks);
- record-keeping requirements; and,
- maintaining and following policies and procedures to drive compliance with these rules.

Money laundering regulations apply to cash transactions **greater than 10,000 euros**.

The **Proceeds of Crime Act 2002 (POCA)** defines a number of substantive money laundering offences, including:

- concealing, disguising, converting and removing criminal funds;
- failing to report suspicious activity to the UK's Financial Intelligence Unit (FIU), which is based in the NCA; and
- tipping-off a suspect about a police investigation Breaches of POCA can be subject to criminal prosecution.

Unlike the money laundering regulations, the Proceeds of Crime Act **applies to all transactions** – cheques, cash, bank transfers, property and equipment to individuals or agents or third parties.

LTE Group is a statutory corporation established under the Further and Higher Education Act 1992 (statutory instrument 2008 No. 1418). LTE Group is an exempt charity for the purposes of Part 3 of the Charities Act 2011.

As stated in the 2020 'National risk assessment of money laundering and terrorist financing':
'[c]harities are not subject to the money laundering regulations but they, their trustees, employees and volunteers are subject to the Proceeds of Crime Act (POCA) and terrorism legislation'.

This includes 'exempt' charities and therefore the Group is required to comply with the Proceeds of Crime Act 2002, but **not** with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017).

However, given that the Group is committed to the highest level of openness, integrity and accountability, both in letter and in spirit, the Group has due regard for MLRs 2017's principles and guidance (insofar as they apply to the further education and charity sectors).

This policy covers all the Group's subsidiaries, except for any subsidiaries who are required to comply with Money Laundering Regulations 2017 (for example if a subsidiary has been granted permissions by the Financial Conduct Authority), for whom a separate policy will be produced.

Money Laundering: Offences and Penalties

As per 'The Code for Crown Prosecutors', money laundering offences are found in **Part 7 of Proceeds of Crime Act 2002 ('POCA')**.

Money laundering offences and penalties that **apply** to LTE Group include:

POCA Section	Offence	Penalty
327	Concealing, disguising, converting, transferring or removing criminal property from England and Wales.	A person convicted of an offence under any of these sections is liable to imprisonment for 14 years, a fine, or both.
328	Arranging, or becoming concerned in an arrangement, which the person who knows, or suspects, or facilitates (by whatever means), the acquisition, retention, use or control of criminal property by or on behalf of another person.	
329	Acquiring, using or having possession of criminal property.	
333	Making a disclosure to a person which is likely to prejudice a money laundering investigation (**"tipping off"**).	A person guilty of an offence under this section is liable on conviction on indictment to imprisonment for a term exceeding 2 years, or to a fine, or to both.

Money laundering offences and penalties that **do not apply** to LTE Group, but to which LTE Group will pay due heed include:

Ref	Offence	Penalty
PCOA Section 330	Having reasonable grounds for knowing or suspecting that a person is engaging in money laundering but fails to disclose to a nominated officer as soon as is practicable. **Note:** Whilst this applies to the regulated sector only, LTE Group has implemented a process to enable colleagues to promptly report any concerns. *	Maximum penalty on indictment of up to 5 years imprisonment.
MLRs - Reg 86	Regulation 86 applies to a person who contravenes a 'relevant requirement'. The relevant requirements include: - Risk assessment by relevant persons - Policies, controls and procedures - Customer due diligence	Under Regulation 86, a person who contravenes these requirements is liable, on conviction on indictment, to imprisonment for a term not exceeding two years, to a fine, or to both. Where the person has taken **all reasonable steps** and exercised **all due diligence** to avoid committing the offence, that person **will not be guilty** of an offence.

Money Laundering: Other Consequences

If an act of money laundering took place and it was deemed that LTE Group did not have adequate procedures in place to guard against money laundering, or had assisted with money laundering, or had tipped-off a money launderer, there would be more repercussions than just the penalties set out in the UK Anti-Money Laundering (AML) framework. These could include:

- Reputational damage
- Potential loss of funding
- Costly legal action
- Potential loss of morale within the Group

Failure to prevent money laundering can also cause practical difficulties, as the National Crime Agency (NCA) can apply to freeze bank accounts, if they believe the account(s) may contain the proceeds of criminal conduct.

Money Laundering: LTE Group Risk Review

The **2020 'National risk assessment of money laundering and terrorist financing'** categorises the education sector within non-profit organisations (pages 124 to 130), and has given this sector the following Risk Scores for both 2017 and 2020:

- 2017 Money Laundering Risk Score – **Low**
- 2017 Terrorist Financing Risk Score – **Low**

- 2020 Money Laundering Risk Score – **Low**
- 2020 Terrorist Financing Risk Score – **Low**

The report states:
'*Consistent with the findings of the previous NRA, this NRA assesses that the NPO sector is not attractive for money laundering and assesses the risk to be **low***.'

As the Group is not required to comply with MLRs 2017, it is **not mandatory** for the Group to perform a money laundering risk assessment.

However, given that the Group is committed to best practice, and in order to inform the control environment, a high-level risk assessment has been made.

This assessment has identified the following risks and mitigations:

Risk	Mitigation
Cash transactions	Across the Group, the amount of cash transactions is low and for small amounts only (e.g. refectories takings). As noted below, the Group's policy is that no cash is accepted as payment for tuition fees. Therefore, this is deemed to be a low-risk area, and this risk continues to decrease as the Group works towards going cashless.
Tuition fees paid by private individuals	The Group's policy is that no cash is accepted as payment for tuition fees. This risk is thereby eliminated.
Requests for refunds / overpayments	The Group receives minimal overpayments. Any repeated overpayments from a single customer would stand out and would be identified as part of the monthly reconciliation process (which identifies credit balances and payments that can't be allocated). Once an overpayment has been identified and investigated, if it is deemed to be genuine, then the Group's policy is to return the payment using the original pay method. The only exception to this would be if the payment was made by card more than 6 months ago, as it would not then be possible to return this by card. In this instance, proof of bank account details in the same name would be requested from the learner. Subject to a beneficiary check made by the Group's bank, payment would then be returned to the learner's bank account.
Donations received	Donations could be exploited for money laundering purposes if the Group received a donation from a suspicious source, or if the donor subsequently sought the return of the funds. This is deemed to be a low-risk area, as the Group rarely receives donations. Should a donation be received, the appropriate identity checks would be made prior to acceptance, to ensure that the source of funds was legitimate and given for exclusively charitable purposes.
Overseas Students	The Manchester College does not currently deliver education overseas. One of the Group's subsidiaries, Total People, does have overseas learners, but as this company has limited FCA permissions, a separate risk assessment will be performed, and policy produced.

Overall, the outcome of this assessment is that the risk of the Group being party to money laundering is deemed to be **low**.

In addition to the reasons given in the table above, it is also worth noting that approximately 80% of the Group's funding is a mix of government (ESFA and Ministry of Justice) and devolved authority (GMCA) funding, as opposed to private individuals, which again reduces the risk of the Group being party to money laundering.

Statement of Policy: Framework

1. LTE Group **prohibits any form of money laundering**. No colleague, or associated person, may engage in any form of money laundering (either in the UK or abroad) with regard to activity carried out within, or on behalf of, the Group.

2. At the outset of any business relationship (and as appropriate thereafter), LTE Group's **zero-tolerance stance on money laundering**, must be communicated to all suppliers, contractors and business partners.

3. All LTE Group colleagues, associated persons and members of the LTE Group Board are responsible for remaining alert and vigilant to the risk of money laundering, and for protecting the reputation of LTE Group.

4. All LTE Group colleagues, and associated persons, **must promptly complete**, as and when issued, any Group **mandatory money laundering training**.

5. LTE Group colleagues or associated persons **must not** do business with anyone they suspect of taking part in any activity, knowingly or unknowingly, which they regard as linked with potential money-laundering.

6. If any LTE Group colleague, or association person, knows, suspects, or has reasonable grounds for thinking or suspecting that a person is engaged in money laundering or terrorist financing, they **must not, at any time or under any circumstances,** voice any suspicions to the person(s) who are suspected of money laundering.

7. If any LTE Group colleague, or association person, knows, suspects, or has reasonable grounds for thinking or suspecting that a person is engaged in money laundering or terrorist financing, they **must immediately pause the transaction** and **report their suspicions** to the Money Laundering Reporting Officer (MLRO), in accordance with the **Money Laundering Response Plan** (see Appendix 1) and via the **Suspected Money Laundering Reporting Form** (see Appendix 2).

8. 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.

9. Once any LTE Group colleague, or association person has reported their suspicions, then any instructions provided by the Money Laundering Reporting Officer (MLRO) and/or Money Laundering Compliance Officer (MLCO) must be followed.

10. Cash transactions are more susceptible to money laundering, and therefore, where possible, cash transactions should be avoided. If they cannot be avoided, to mitigate the risk of money laundering, stringent controls should be applied. Therefore, **no cash payment greater than £2,500 can be accepted**, *unless* the Money Laundering Compliance Officer (MLCO) grants prior approval.

11. Cash **must not** be accepted as payment for tuition fees. Tuition fees can only be paid in line with the relevant business unit's tuition fee policy.

12. Tuition fee refunds can only be made in line with the relevant business unit's tuition fee policy. Refund payments, and any other form of return of overpayments, can only be made following

budget holder approval, and only once sufficient steps have been taken to determine that the refund is genuine and that the original source of funds was legitimate.

13. Refunds and return of overpayments can only be made to the original payer, and, where possible, must be made using the original method of payment. If the original payment was made by card more than 6 months ago, then proof of bank account details in the same name must be requested from the learner, and the payment made via bank transfer (subject to a beneficiary check).

14. If the original payment has been received from abroad, the refund can only be made to the original, foreign bank account and must not be made to a UK bank account (even if the account is in the same name).

15. If a genuine overpayment is made by a learner or a trade customer, then every effort must be made to return the overpayment. If a genuine overpayment is not promptly investigated and returned, then this could be perceived as dishonest behaviour, which in turn could amount to theft. In turn, the Group would therefore be in possession of the proceeds of its crime, which is considered a money laundering offence.

16. Donations can only be received if the identity of the donor is known, if the source of funds has been verified, and if the donation is given for exclusively charitable purposes. A donation **must** be refused if the donor is on the UK's sanctions list.

17. If the Group is subject to a cyber ransomware attack, the ransom demanded **must not** be paid, either by the Group or the Group's insurance company. This is because paying a ransom is deemed to be transferring criminal proceeds and under anti-money laundering legislation is considered a crime.

18. Accurate financial records and reporting must be maintained and regularly reviewed. Records must be retained in line with the Group's retention schedule.

Statement of Policy: Use of Third-Party Representatives

The definition of a third-party representative is broad, and could include an agent, a distributor, a contractor, a supplier an advisor, a consultant, a subsidiary or a joint venture partner.

Third-party representatives who operate on LTE Group's behalf **must**, at all times, act in accordance with this policy. Therefore, all third-party representatives must be selected with care, and all agreements concluded under terms that are in line with this policy.

Third-party representatives **must** keep proper books and records, which are available for inspection by LTE Group, its auditors, or any investigating authorities.

Colleagues are responsible for the evaluation of each of their third-party relationships, and for determining whether or not there are any specific risks. Where specific risks are identified, colleagues **must**:

- evaluate the background, experience and reputation of the third-party;
- understand the services to be provided, and methods of compensation and payment;

- evaluate the rationale for engaging the third-party;
- take reasonable steps to appropriately monitor the transactions of third parties; and
- ensure there is a written agreement in place which acknowledges the third-parties understanding and compliance with this policy.

Proven or Attempted Money Laundering, Failure to Report and 'Tipping-Off': Internal Sanctions

To act as a deterrent to others, a main objective in any anti-money laundering investigation will be the punishment of the perpetrators (if the incident involves a colleague or student).

LTE Group will instigate disciplinary procedures against any colleague or student who is proven to be involved in money laundering. LTE Group will normally involve the police and pursue the prosecution of any such individual.

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

LTE Group will also instigate disciplinary procedures against any colleague who:

- has reasonable grounds for knowing or suspecting that a person is engaging in money laundering but fails to disclose to a nominated officer as soon as is practicable; or
- is proven to have made a disclosure to a person which is likely to prejudice a money laundering investigation ("tipping off").

Proven or Attempted Money Laundering, Failure to Report and 'Tipping-Off' – Third Parties Sanctions

LTE Group reserves the right to terminate its contractual arrangements with any third-party providing services for or on behalf of the Group where there is reasonable evidence that they/their colleagues have:

- committed, or attempted to commit money laundering;
- have had reasonable grounds for knowing or suspecting that a person is engaging in money laundering but have failed to disclose to the relevant authority; or
- have been proven to have made a disclosure to a person which is likely to prejudice a money laundering investigation ("tipping off").

Statement of Responsibility – LTE Group Board & Chief Executive Officer

As set out in grant funding agreements and contracts with ESFA, LTE Group is responsible for establishing and maintaining an adequate system of internal control, to ensure compliance, and to prevent and detect irregularities, including money laundering.

Anti-money laundering obligations are also imposed due to the Group's charitable status. The LTE Group Board are therefore obliged to ensure that sufficient safeguards are in place (via anti-money laundering policies, controls and procedures) to protect the Group from financial crime.

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 managing the Group's risks, including money laundering, and 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 contract between LTE Group and the ESFA. He is also responsible for reporting to the Group Board any material weaknesses or breakdowns in internal control.

The CEO is accountable to the Group Board and should ensure that responsibilities are assigned across the company for implementing the anti-money laundering programme. The CEO is also responsible for setting the tone from the top and for ensuring that all colleagues feel protected when carrying out their official duties, and that they would feel confident in raising any legitimate concerns.

Statement of Responsibility – Money Laundering Compliance Officer (MLCO)

The Chief Executive Officer has designated the **Chief Financial Officer** to be the **Money Laundering Compliance Officer (MLCO)**.

The Money Laundering Compliance Officer is responsible for ensuring that LTE Group is compliant with the UK anti-money laundering (AML) legislation with which it must comply, and that due regard is also given to any other relevant UK AML legislation. This is achieved through implementing anti-money guidelines and through the monitoring of compliance with this policy.

The Money Laundering Compliance Officer is responsible for:

- implementing financial controls, including, where appropriate, mandatory training, to prevent and detect money laundering through the Group's accounts;

- ensuring that accurate financial records and reporting are maintained, regularly reviewed and retained in line with the Group's retention schedule; and for

- regularly reviewing the effectiveness of the Group's anti-money laundering arrangements and for implementing improvements as appropriate.

Statement of Responsibility – Money Laundering Reporting Officer (MLRO)

As an exempt charity the Group is required to comply with the Proceeds of Crime Act 2002, but **not** with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017).

Therefore, as this is a MLRs 2017 requirement, the Group is **not** obliged to appoint a Money Laundering Reporting Officer (MLRO) but has chosen to do so voluntarily.

The Chief Executive Officer has designated the **Company Secretary & General Counsel** to be the **Money Laundering Reporting Officer (MLRO)**.

The Money Laundering Reporting Officer (MLRO) is responsible for:

- receiving notifications of suspected acts, or attempted acts, of money laundering from LTE Group colleagues and associated persons via the Suspected Money Laundering Reporting Form (see Appendix 2);

- ensuring that when such notifications are received, that the allegations are immediately investigated in line with the procedures and timeframes set out in the Money Laundering Response Plan (see Appendix 1);

- in instances when they believe there are reasonable grounds for suspicion that money laundering offences are taking place in connection with the Group, making any required external reports of suspicious activity (in accordance with the Money Laundering Response Plan); and

- maintaining a suspected money laundering register of all suspected money laundering offences of which they have received notification.

If an act of money laundering is proven, the MLRO must inform the chair of the Audit and Risk Committee, external auditors and internal auditors 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 (or less than £10,000 if unusual, novel, complex or there may be public interest).

Where the MLRO considers a potential breach has taken place, they are also obliged to report serious incidents to the Office for Students (OfS).

In discharging their responsibilities, the MLRO must take all necessary precautions to avoid 'tipping off'.

Statement of responsibility – Audit and Risk Committee

The Audit and Risk Committee are responsible for:

- overseeing the corporation's policies on and processes around money laundering;

and for ensuring:

- the proper, proportionate and independent investigation of all allegations and instances of money laundering;
- that investigation outcomes are reported to the Audit and Risk Committee;
- that the Group's obligations with regard to the external reporting of instances of money laundering, for example to the Police, are properly discharged;
- that the external auditor and internal auditor are informed of investigation outcomes and other matters of money laundering, and that appropriate follow-up action has been planned/actioned;
- that all significant cases (exceeding £10,000 in value) of money laundering are reported to ESFA as soon as possible; and that
- risks around money laundering have been identified and controls put in place to mitigate them.

Statement of Responsibility – Income and Credit Control Team

The Income and Credit Control team are responsible for ensuring that any refunds made to students or customers are made in accordance with 12 to 15 in the statement of policy above.

Statement of Responsibility – Line Managers

LTE Group Line Managers are responsible for:

- implementing this policy in respect of money laundering;
- identifying, and assessing the scale, of common types of money laundering risk in their area and **alerting the Money Laundering Compliance Officer (MLCO)** if they identify any areas of concern;
- ensuring all of their team members have completed all mandatory anti-money laundering training;
- where relevant, ensuring that anti-money laundering controls are constantly applied and that procedures are being followed, through routine checks and monitoring;

- where relevant, identifying and investigating any areas in which anti-money laundering controls are not being uniformly applied, and taking remedial action if required;

- setting a good example – line managers should comply, and be seen to comply, with all controls;

- **promptly** reporting to the **Money Laundering Reporting Officer (MLRO)**, if a member of their team raises any concerns about suspected money laundering; and,

- providing support, as and when required, to investigations of alleged acts of money laundering.

The Chief Financial Officer and Internal Audit can offer advice and support to line managers regarding the implementation and documentation of effective systems of internal control.

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;

- completing all mandatory anti-money laundering training;

- remaining alert and vigilant to the risk of money laundering;

- protecting the reputation of LTE Group;

- applying the internal controls, and rules and regulations that are designed to deter, prevent and detect money laundering;

- **pausing any financial transaction** if they have reasonable grounds for thinking or suspecting that the other party is engaged in money laundering or terrorist financing;

- ensuring that they do not **at any time or under any circumstances,** voice any suspicions to the person(s) who are suspected of money laundering;

- **immediately** reporting all legitimate concerns about suspected money laundering in accordance with the Money Laundering Response Plan; and

- not allowing their 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.

Statement of Responsibility – External Organisations

All external organisations who deal with LTE Group, must:

- operate within the law and any specific agreements or contracts;
- comply with LTE Group's Anti-Money Laundering Policy; 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 money laundering; this is the responsibility of LTE Group management.

Internal Audit Plan
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 money laundering.

For example, the Internal Auditor can:

- regularly review anti-money laundering 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 money laundering risk;
- help determine the appropriate response to suspected money laundering and to support any investigation taking place; and,
- facilitate corporate learning on money laundering, money laundering prevention and the indicators of money laundering.

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. Systems should be tested to ensure that the risk, both internal and external, is minimised, and the Internal Auditor should be alert to any control weaknesses that could allow money laundering to occur.

Reporting to the National Crime Agency (NCA)
The responsibilities of statutory auditors in the UK in respect of money laundering are set out in Practice Note 12 (Revised), issued by the Auditing Practices Board of the Financial Reporting Council. Under relevant legislation including the Proceeds of Crime Act (POCA), auditors are required to report to the National Crime Agency where:

- they know or suspect, or have reasonable grounds to know or suspect, that another person is engaged in money laundering;

- they can identify the other person or the whereabouts of any of the laundered property or that they believe, or it is reasonable to expect them to believe, that information that they have obtained will or may assist in identifying that other person or the whereabouts of the laundered property; and
- the information has come to the auditor in the course of its regulated business.

In discharging their responsibilities, auditors must take all necessary precautions to avoid 'tipping off'.

Statement of Responsibility – External Auditor

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

Financial Statements Audit
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 (including the potential impact of money laundering) or error.

If it is suspected that money laundering has occurred the auditor would need to apply the concept of materiality when considering whether the auditor's report on the financial statements needs to be qualified or modified, taking into account whether:

- the crime itself has a material effect on the financial statements;
- the consequences of the crime have a material effect on the financial statements; or
- the outcome of any subsequent investigation by the police or other investigatory body may have a material effect on the financial statements.

Reporting to the National Crime Agency (NCA)
The responsibilities of statutory auditors in the UK in respect of money laundering are set out in Practice Note 12 (Revised), issued by the Auditing Practices Board of the Financial Reporting Council. Under relevant legislation including the Proceeds of Crime Act (POCA), auditors are required to report to the National Crime Agency where:

- they know or suspect, or have reasonable grounds to know or suspect, that another person is engaged in money laundering;
- they can identify the other person or the whereabouts of any of the laundered property or that they believe, or it is reasonable to expect them to believe, that information that they have obtained will or may assist in identifying that other person or the whereabouts of the laundered property; and
- the information has come to the auditor in the course of its regulated business.

In discharging their responsibilities, auditors must take all necessary precautions to avoid 'tipping off'.

Appendix 1 – Money Laundering Response Plan

Introduction

The Money Laundering Response Plan sets out LTE Group's procedures for ensuring that all allegations and reports of money laundering are properly and fairly investigated, and that immediate and effective action is taken.

Reporting to the National Crime Agency (NCA)

As an exempt charity, the Group is required to comply with the Proceeds of Crime Act 2002, but **not** with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017).

As per the Government guidelines on reporting suspicious activities in relation to money laundering, it is **only** organisations who are registered for money laundering supervision who are obliged to disclose their suspicions to the National Crime Agency (NCA) via a Suspicious Activity Report (SAR).

Organisations who are not registered for money laundering supervision are instead only required to send a report of breaches of the money laundering regulations to the HMRC Fraud Hotline.

However, submitting a SAR is best practice and protects the Group, the colleagues involved and UK financial institutions from the risk of laundering the proceeds of crime. Therefore, if there are reasonable grounds for suspecting that a money laundering offence has been attempted or committed, then the Group will voluntarily submit a SAR.

Making a Notification of Suspected Money Laundering

If any LTE Group colleague, or association person, knows, suspects, or has reasonable grounds for thinking or suspecting that a person is engaged in money laundering or terrorist financing, they **must immediately pause the transaction** and **report their suspicions** to the Money Laundering Reporting Officer (MLRO) using the **Suspected Money Laundering Reporting Form** (see Appendix 2).

As much details as possible should be included in the form, as even a detail that might seem trivial or irrelevant could become a valuable piece of information.

Receipt of a Notification of Suspected Money Laundering

Regardless of the value of the amounts involved, **all** alleged instances of money laundering should be reviewed by the Money Laundering Reporting Officer (MLRO).

Within 24 hours of the incident being reported, the MLRO should ensure all the details of the suspected money laundering have been recorded and verified with the colleague (or associated person) who has made the report.

The colleague (or associated person) must follow any subsequent directions from the MLRO and must not make any further enquiries themselves into the matter. Additionally, if, due to becoming suspicious, they have paused a financial transaction, then they must not proceed with this transaction without authorisation from the MLRO.

At no time and under no circumstances should the colleague (or associated person) voice any suspicions to the person(s) they suspect of money laundering, nor should they discuss this matter with any colleagues other than the MLRO.

Review of a Notification of Potential Money Laundering

Where possible, the Money Laundering Reporting Officer (MLRO) should then immediately alert the Money Laundering Reporting Officer (MLCO) that a notification has been received and should meet with her/him to discuss whether:

- there are prima facie grounds for suspicion that a money laundering offence has been attempted or committed; and therefore,

- whether there is a requirement to make an external disclosure to the Police and other relevant external organisations, such as HMR&C, the National Crime Agency (NCA), the ESFA, and the Office for Students (OfS); and

- if the suspicious transaction has not yet taken place, whether the transaction should be suspended *.

* If it's not practical or safe to suspend the transaction, the Money Laundering Officer (MLRO) should submit a SAR as soon as possible after the transaction is completed.

Unless there are any grounds for concern that any of the following may have any involvement in the incident, the Money Laundering Reporting Officer (MLRO) may also wish to consult:

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

Outcome - No Grounds for Concern

If the Money Laundering Reporting Officer (MLRO) determines that there are no grounds for concern, then the matter may be dismissed, and consent given to proceed with any suspended transaction(s).

The MLRO is responsible for communicating this decision to the colleague (or associated person) who reported the suspected money laundering.

The colleague (or associated person) 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 Money Laundering Reporting Officer (MLRO) determines that there are grounds for concern, then the MLRO must promptly report the matter to the National Crime Agency (NCA), using their SAR online system (Welcome to the NCA SAR Online System (ukciu.gov.uk)).

The MLRO will commit a **criminal offence** if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering, and they do not disclose this as soon as practicable to the NCA.

SARs are reports detailing the knowledge or suspicion a reporter has of money laundering or terrorist financing and are **not** crime reports. Therefore, the MLRO should also consider whether they also need to make a crime or a fraud report to the Group's local police service on 101 or Action Fraud on 0300 123 2040.

Again, depending on the nature and severity of the incident, the Company Secretary & General Counsel should consider whether the suspected money laundering offence should be reported directly to any other external parties, such as the ESFA and the OfS. Please see 'Other Reporting Requirements' below.

Submitting a Suspicious Activity Report (SAR) to National Crime Agency (NCA)

The NCA receives and analyses SARs and uses them to identify the proceeds of crime. It counters money laundering and terrorism by passing on important information to law enforcement agencies so they can take action.

Reporters of SARs will **not** routinely be provided with updates on their SARs and may only become aware of the existence of operational activity if law enforcement then requests further information.

The MLRO must consider whether the Group requires defence against money laundering charges from the NCA before proceeding with a suspicious transaction or activity.

If the MLRO receives a reply from the NCA within 7 working days and believes that the activity has been correctly reported, they can choose to assume a defence is granted.

If the MLRO receives a reply that says the Group does not have permission to proceed with the transaction, the NCA have a further 31 calendar days to take action.

If the MLRO has not heard from the NCA after the 31 days, they can then decide whether to proceed with the transaction, as to do so would not be committing an offence. However, the MLRO should consider factors such as financial exposure, value for money, reputational risk and propriety, and should consult with the CFO and CEO as appropriate.

However, the 31 day period does not apply to terrorist financing cases, in which instance the Group would not have a defence until the NCA granted the request.

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 as soon as possible when the amounts are significant, that is **exceeding £10,000** in value, (or less than £10,000 if unusual, novel, complex or there may be public interest).

- 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 incident, other external bodies may need to be informed, e.g. HM Revenues and Customs.

- If the incident constitutes 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.

Suspected Money Laundering Register

The Money Laundering Reporting Officer (MLRO) is responsible for maintaining a suspected money laundering register.

For every suspected incident of money laundering, details will be recorded on the register of:

- the date the incident was reported
- a description of the incident
- whether or not it was determined there were ground for concern
- the date (if reported) the incident was reported to the NCA
- details of any correspondence with the NCA
- if applicable, whether a defence was granted and whether the transaction proceeded
- the outcome of any NCA investigation (of which the MLRO is aware)
- the cost and/or adverse impact on LTE Group
- if a colleague or 3rd party was involved in the offence, details of any internal or external sanctions applied
- details of any Police involvement
- date reported to the Audit and Risk Committee
- details of any communications to other external authorities
- actions taken to improve the control environment

The record of each incident should be made promptly and should be capable of providing an audit trail during any subsequent investigation.

Appendix 2 – Suspected Money Laundering Reporting Form

Suspected Money Laundering Reporting Form *Please complete and send this to the Money Laundering Reporting Officer (MLRO) using the form below.* This form should be completed **the same day** as the information came to your attention, as **if you do not do so you may be personally liable to prosecution**.	
Name & Role:	**Business Unit:**
Contact Details:	
DETAILS OF SUSPECTED OFFENCE [Please provide as much detail as possible]	
Name(s), address(es) and full available details of person(s) involved, and/or companies involved, and/or any other colleagues involved, including relationship with the Group:	
Suspected type of money laundering activity with exact reasons as to why you are suspicious:	
Full details of nature, value and timing of any transaction(s) and nature of each person(s) identified above involvement in the transaction(s):	
The dates of any transaction(s), where they were undertaken, how they were undertaken and the likely amount of money or assets involved:	
Details of any enquiries you may have undertaken to date:	
Have you discussed you suspicions with anyone? (* see below) And if so, on what basis?	
Is any aspect of the transaction(s) outstanding and requiring consent to progress?	
Any other relevant information that may be useful?	

MLRO contact details: **Name:** Lorna Lloyd-Williams **Role:** Company Secretary & General Counsel **Email address:** lloydwilliams@ltegroup.co.uk **Phone number:** 0161 674 3683
** Please **do not** discuss the content of this report **with anyone you believe to be involved in the suspected money laundering activity described**. To do so may constitute a tipping off offence, which carries a maximum penalty of 5 years' imprisonment and/or an unlimited fine.*

Owner: Chief Financial Officer
Group Audit Committee
Date of approval: 18th July 2023
Review cycle: three years