The LETTA Trust

Anti-Fraud Policy

Approved and adopted on:	Spring 2026	**To be reviewed:**	Spring 2027
Reviewed by:	TB Audit & Risk	**Signed:**	

Contents

1. Introduction

The Letta Trust is committed to ensuring that it demonstrates the highest standards of business conduct and that it maintains an honest and open environment within the Trust and its schools. It is also committed to promoting an anti-fraud culture, the prevention and detection of fraud and irregularity and the investigation of any such cases. Any apparent fraud or financial irregularity will be investigated and appropriate action will be taken where there is evidence of such. The recovery of money and/or assets from individuals found to be guilty of participating in fraudulent activity will be pursued (through formal criminal and civil action where appropriate). All staff have a duty to:

- Protect the assets of the Trust and its schools
- Report all reasonably held suspicions of fraud or irregularity
- Cooperate with any investigation

2. What is fraud?

Fraud is a deliberate use of deception carried out in order to gain an unfair advantage or to disadvantage another. It may involve the misuse of funds or other resources, or the supply of false information.

Under the Fraud Act 2006, the offence of fraud can be committed in one of the following ways:

- By false representation
- By failing to disclose information
- By abuse of position
- By the possession, making or supplying articles for use in frauds
- By obtaining services dishonestly with intent to avoid payment

Common types of fraud include theft, bribery, corruption, fictitious invoices, falsification of invoices and credit card fraud. Cybercrime and email hacking enable people to illegally gain access to personal information such as account numbers, passwords and dates of birth.

A crime is committed with the actual intention to defraud not its realisation.

3. Other Irregularities

Other irregularities could apply to the Trust as well as individual schools, and includes:

- Failure to observe the Trust's Financial Regulations, policies and procedures
- Breach of our Funding Agreement with the DfE

- Breach of the requirements of the Academies Trust Handbook
- Spending grant income in ways inconsistent with the purposes for which it was intended
- Engaging in novel, contentious or repercussive transactions without prior DfE approval

4. Preventing fraud

The LETTA Trust aims to prevent fraud from happening by developing an effective anti-fraud culture. The CEO and CFO are responsible for:

- Promoting an awareness of fraud through staff training
- Encouraging employees to be vigilant and to report any suspicions of fraud
- Ensuring effective screening during recruitment
- Confirming contacts and routes for staff to report suspicions of fraud, including using the whistleblowing policy
- Assessing the Trust's overall vulnerability to fraud using the anti-fraud checklist (appendix 1)
- Identifying the area's most vulnerable to fraud risk using the list of fraud indicators
- Evaluating the level of fraud risk
- Establishing cost-effective internal systems of control
- Continuously evaluating the effectiveness of anti-fraud measures
- Ensuring there is a carefully designed and consistently operated management procedure, in particular the financial policies and procedures within the Trust's Financial Regulations
- Ensuring there are proportionate controls and plan to take appropriate action where a cyber security incident has occurred
- Ensure that management procedures for the Trust and within schools, are effective and that staff receive training in their operation
- Undertaking a 'lessons learned' exercise if fraud occurs

Leadership

- Key determinants of the standards of behaviour in The Letta Trust and its schools are the standards observed by senior members of staff and the policies and approach to their enforcement promoted by senior staff
- The Trust Board and its committees and senior managers of the executive, ensure that their behaviour is always demonstrably selfless, impartial and consistent with the public service values of probity and accountability

Internal Scrutiny

- Internal Scrutiny (provided by Baxter & Co) provides independent assurance on the processes and controls put in place by management to prevent or detect fraud and irregularity or to manage the risk of fraud and irregularity

- The Internal Auditors may also provide advice on, lead or conduct special investigations into suspected fraud, irregularities, misconduct or alleged impropriety. Fraud investigations will not be undertaken without the requisite skills, knowledge and expertise as this may compromise a fraud investigation or a criminal case
- Internal scrutiny will also include an assessment of the Trust's vulnerability to fraud and a review of the effectiveness of the Trust's anti-fraud and cyber security controls

External Audit

- The External Auditors (Craufurd Hale LLP) provide independent oversight of the financial controls and activities within the Trust and its schools as part of their work in auditing the year-end financial statements

Department for Education (DfE)

- The DfE carries out periodic funding audits and financial management reviews. They also conduct or commission investigations into suspected fraud and irregularity and they publish reports on the outcome of such investigations

5. Detection

Internal Management Systems

- Effective management systems are imperative if fraud is to be detected rapidly; the central trust team carries out a systematic review of every transaction to minimise the risk of processing an irregular transaction
- Detective checks and balances are designed into systems and applied consistently. This includes segregation of duties, reconciliation procedures and review of management accounting information

Internal or External Audit Reviews

- The work of internal and external auditors or inspectors may result in the detection of suspected fraud and irregularity or may suggest improvements in controls to help prevent and detect any irregularities

Cyber security

- Prevention of unauthorised access to programmes & data, including access by hackers
- Regular backing up of information & storage of backed up information away from its normal work place in a secure, fire protected environment
- Security of computer & system manuals & other unique information
- Control of passwords & data links
- Virus protection software which is regularly updated
- Utilising the **NCSC's Cyber Security Evaluation Tool** or similar to benchmark resilience

Potentially Suspicious Behaviour

- Staff members who have committed serious financial irregularities may attempt to conceal this by taking few holidays, regularly working alone, late or at weekends, being resistant to delegation or resenting questions about their work. The DfE's 'Fraud Indicators' document (appendix 2) may be helpful to refer to where concerns may exist. If in doubt, staff members should report their suspicions anyway

Reporting

- Staff report any suspicions of fraud or irregularity to the CEO, the Chair of Governors or the Chair of Trustees provided they are supported by at least one piece of reliable information or evidence and they are made in good faith
- Reporting suspicions using the Trust's Whistleblowing Procedure

6. Investigation of Suspected Fraud and Irregularity

In order to protect the Trust and those accused of suspected fraud and irregularity, initial enquiries will be made to decide whether an investigation is appropriate .In cases of suspected fraud or financial crime, an initial strategy meeting involving the CEO, Chair of Trustees and CFO will take place at the earliest opportunity to determine the response.

Each case will be different and the approach taken will be dependent upon the circumstances, nature and seriousness of the allegations and the potential remedies being sought. The course of action to be taken is likely to be one or more of the following:

- An investigation conducted by management, the Internal Scrutiny providers , or through the disciplinary process
- Referral to the police, the DfE Investigations Team or other investigative bodies
- Referral toan appropriate professional body or the external auditor
-
- Reporting to the DfE any instances of fraud exceeding £5,000 (individually or cumulatively in a financial year), or any systematic or unusual fraud regardless of value.
- Notifying the DfE of any regular occurrences of low value theft regardless of value (paragraph 6.10 of the Academies Trust Handbook)
- Reporting all significant cyber-attacks to Action Fraud and the NCSC. The DfE must be notified of any cyber-related financial loss exceeding £5,000. Note prohibition on ransoms: The Trust must not pay any cyber ransom demands. Payment is a "novel and contentious" transaction and is strictly prohibited by the DfE
- The Trust will not enter into any settlement or 'ex-gratia' payment agreements with individuals under investigation for fraud or financial irregularity without prior express approval from the DfE

The following information is required for the reporting & investigation of fraud:

- Full details of the event(s) with dates
- The financial value of the loss
- Measures taken to prevent recurrence
- Whether it was referred to the police (and if not why)
- Whether insurance or the RPA have offset any loss

When a decision is made to investigate the matter internally, the case will be referred to an individual who has the appropriate expertise and seniority to plan and undertake the preliminary fact finding and/or formal investigation(s).

The investigation is conducted in a professional manner, in accordance with relevant procedures.

The purpose of an investigation is to establish the facts associated with the concerns or allegations in order to determine whether or not there is a case to answer.

The Investigating Officer will adopt a holistic approach examining the case from all angles, collecting evidence from management, employee and organisational perspectives. The Investigating Officer will interview all relevant people and analyse any related documentation in order to determine the facts and relevant mitigating circumstances.

Some investigations (e.g. involving fraud or financial crime) may require the use of technical or specialist expertise in which case the Internal Auditors (Baxter & Co) will be employed as the Investigating Officer or to contribute to the investigation.

The CFO or CEO will inform the Chair of the Trust Board and the Chair of the Audit Committee that an investigation is taking place.

The Investigating Officer will, where possible, quantify any potential or actual financial loss and ensure that steps are taken at an early stage to prevent further loss occurring.

Where the case is sufficiently serious, an individual who is accused of fraud or irregularity may be suspended, with or without pay, while an investigation is underway, in accordance with the Trust's disciplinary procedures.

The CEO should be consulted before any such action is taken. It should be noted that suspension is a neutral act intended to facilitate enquiries, protect the Trust and the individual(s) involved and does not imply any presumption of guilt.

7. Useful resources

- Academies Trust Handbook
-
- ISBL Professional Resources
-
- Whistleblowing for employees
- City of London police: fraud & economic crime
- https://www.ncsc.gov.uk/ National Cyber Security Centre
- Action Fraud
- Chartered Institute of Public Finance & Accountancy (CIPFA) counter-fraud centre
- How to raise a concern about an academy
- NCSC - Cyber Security for School
- DfE Academy Trust Governance Guide

Appendix 1 Anti-fraud checklist

The ten questions below are used to help the Trustees, CEO and CFO to review arrangements for preventing, detecting and dealing with fraud.

1. Are the Trustees, CEO and CFO aware of the risk of fraud and their responsibilities regarding fraud?

2. Is there a 'zero tolerance' culture to fraud in the Trust?

3. Is fraud included within the remit of the Trust's audit committee?

4. Has the role of the Trust's external auditor regarding fraud been established and is it understood?

5. Is fraud risk considered within the Trust's risk management process?

6. Is the Trust's fraud policy regularly reviewed and up to date?

7. Is the fraud policy and 'zero tolerance' culture promoted within the Trust, for example through financial regulations, disciplinary procedures, checks on new staff, induction process, staff training, vetting of contractors?

8. Does the Trust have policies on whistleblowing and declaration of interests and receipt of gifts and hospitality?

9. Does the Trust maintain an up-to-date Register of Interests published on the website and reviewed at every meeting?

10. Does the Trust have appropriate segregation of duties around financial transactions, including, but not limited to, accounting, processing and banking arrangements?

11. Is it clear to whom suspicions of fraud in the Trust should be reported?

12. If there has been any fraud in the Trust has a 'lessons learned' exercise been undertaken?

Appendix 2 Fraud Indicators

This is a list of indicators of potential fraud. These include personal and organisational motives for fraud, possible weakness of governance or internal controls, transactional indicators and possible methods of concealing fraud.

Ref	Issues increasing fraud risk	Mitigating controls	Required improvement
1	**Potential personal motives**		
1.1	Financial motives: ● Personnel believe they receive inadequate pay and/or rewards (recognition, holidays, promotions etc.) ● Individuals' expensive lifestyles (cars, holidays etc.) ● Personal problems (gambling, alcohol, drugs, debt, etc.)		
1.2	Personal motives: ● Disgruntled employee (recently demoted, reprimanded etc.) ● Recent failure associated with specific individual ● Personal animosity or professional jealousy		
1.3	Unusually high degree of competition/peer pressure		
1.4	Undeclared conflicts of interest or related party transactions (business activities with personal friends, relatives or their companies)		

2	Possible organisational motives		
2.1	Financial issues: • Organisation experiencing financial difficulty • Commercial arm experiencing financial difficulty • Organisation has for-profit component • Not-for-profit entity has a for-profit counterpart with linked infrastructure (shared board of governors or other shared functions and personnel) • Organisation under pressure to show results (budgetary, exam results etc.) • Organisation recently suffered disappointment/reverses/consequences of bad decisions • Organisation recently affected by new/changing conditions (regulatory, economic, environmental etc.) • Organisation faces pressure to use or lose funds to sustain future funding levels		
2.2	Tight or unusually tight time deadlines to achieve level of outputs		
2.3	Organisation wants to expand its scope, obtain additional funding		
2.4	Funding award up for continuation		
2.5	Organisation due for a site visit by auditors, Ofsted or others		
2.6	Record of previous failure(s) by one or more organisational areas		

3	**Potential weaknesses in management and governance**		
3.1	Organisation governance lacks clarity and direction		
3.2	Organisation closely identified with one individual		
3.3	Management demonstrates lack of attention to ethical values (eg. Nolan principles, integrity and ethics)		
3.4	Risk management: • Management fails to recognise required levels of competence in high risk areas • Management displays lack of commitment towards the identification and management of risks relevant to the preparation of financial statements (does not consider significance of risks, likelihood of occurrence or how they should be managed) • Management take unnecessary risks		
3.5	Institution lacks policies and communication relating to financial management, individual accountability and best practices e.g. • Procurement • Travel and subsistence • Use of alcohol • Declarations of interest		
3.6	Personnel policies: • Lack of personnel policies and recruitment practices • Institution lacks personnel performance appraisal measures or practices		
3.7	Management is unaware of or displays lack of concern regarding applicable laws and regulations e.g. Companies Acts, Charities Acts, Funding Agreement, Child Protection		
3.8	Sudden change in organisation practice		
3.9	Lack of staff training or fraud awareness		
3.10	Lack of Digital Leadership: Management fails to understand or implement the DfE's "Digital and Technology Standards		
3.11	Lack of a "Defensible" Pay Policy: Board cannot provide documented evidence that executive pay is transparent, proportionate, and justifiable		

4	Potential internal control issues		
4.1	**Internal control**		
4.1.1	Lack of an appropriate organisational and governance structure with defined lines of authority and reporting responsibilities		
4.1.2	Lack of oversight of budget management, including comparison of budgets with actual performance and costs, forecasts and prior performance; no regular reconciliation of control records and lack of proper reporting to governing body		
4.1.3	General lack of management oversight or appropriate level of challenge		
4.1.4	There is inadequate or inappropriate segregation of duties regarding initiation, authorisation and recording of transactions, maintaining custody of assets		
4.1.5	There is a lack of internal, independent monitoring of controls in place; failure to take any corrective actions, if needed		
4.1.6	No mechanism exists to inform management and governors of possible fraud		
4.1.7	Management of information systems is inadequate (no policy on information technology security, computer use and access, verification of data accuracy completeness or authorisation of transactions)		
4.1.8	Accounting systems are inadequate (ineffective method for identifying and recording transactions, no tracking of time periods during which transactions occur, insufficient description of transactions and to which account they should be allocated to, no easy way to know the status of funds on a timely basis, no adequate procedure to prevent duplicate payments or prevent missing payment dates, etc.)		
4.1.9	Purchasing systems/procedures inadequate (poor or incomplete documentation of purchase, payment, receipt; poor internal controls as to authorisation and segregation of duties)		
4.1.10	Previous audits with findings of: • Questioned costs		

	• Evidence of non-compliance with applicable laws or regulations • Weak internal controls • Inadequate management response to any of above • A qualified opinion		
4.1.11	• History of problems • Slow response to past findings or problems • Unresolved findings		
4.1.12	There is insufficient physical security over facilities, assets, records, computers, data files, cash; failure to compare existing assets with related records at reasonable intervals		
4.1.13	**Cyber Security Vulnerability:** No clear strategy for backing up data offline; lack of Multi-Factor Authentication (MFA) on financial systems		
4.1.14	**Ransomware Policy Gaps:** Absence of a policy stating that the trust **must not** pay cyber ransom demands		
4.2	**Transactional indicators**		
4.2.1	Related party transactions with inadequate, inaccurate or incomplete documentation or internal controls (business/research activities with friends, family members or their companies)		
4.2.2	Specific transactions that typically receive minimal oversight		
4.2.3	Transactions and/or accounts • Which are difficult to audit or • Subject to management judgement and estimates		
4.2.4	Payroll (including fringe benefits) system: controls inadequate to prevent an individual being paid twice, or paid for non-delivery or non-existence; or outsourced but poor oversight of starters / leavers and payments		
4.2.5	Travel and subsistence accounts with: • Inadequate, inaccurate or incomplete documentation • Receipts not provided		

	• Variances between budgeted amounts and actual costs • Claims in excess of actual expenses • Reimbursement for personal expenses • Claims for non-existent travel • Collecting duplicate payments		
4.2.6	Credit card accounts with inadequate, inaccurate or incomplete documentation or internal controls such as appropriate authorisation and review		
4.2.7	Consultant/ subcontract agreements which are vague as to • Schedule of work • Time period covered • Rate of pay • Product expected Lack of proof that product or service actually delivered		
4.2.8	Accounts in which activities, transactions or events involve handling of cash or wire transfers; presence of high cash deposits maintained with banks		
4.2.9	Writing large cheques to cash or repeatedly to a particular individual, or excessive or large cash transactions		
4.2.10	Multiple sources of funding with • Inadequate, incomplete or poor tracking • Failure to segregate funds and/or • Existence of pooled funds		
4.2.11	Unusual, complex or new transactions, particularly if occur at year end, or end of reporting period		
4.2.12	Accounts with large or frequent shifting of budgeted costs from one line item to another without adequate justification		
4.2.13	Transactions and accounts operating under time constraints		
4.2.14	Cost sharing, matching or leveraging arrangements where industry money or other donation has been put into a foundation (as in a foundation set up to receive gifts) without adequate controls to determine if money or equipment has been spent/used and whether it has gone to allowable		

	costs and at appropriate and accurate valuations; outside entity such as foundation provided limited access to documentation		
4.2.15	Assets and inventory are of a nature to be easily converted to cash (small size, high marketability, lack of ownership identification, etc.) or easily converted to personal use (cars, houses, equestrian centres, villas etc.)		
4.2.16	**Mandate/Bank Detail Changes:** Requests to change supplier bank details via email without independent "call-back" verification to a known number		
4.2.17	**Unusual Spending on "Procurement Cards":** Increase in small, rounded-sum transactions or purchases that bypass the standard purchase order (PO) system		
4.3	**Record keeping and banking**		
4.3.1	Records maintained are inadequate, not updated or reconciled. Examples: • Missing documents • Documents are copies, not originals • Documents in pencil • Altered documents • False signatures/incorrect person signing		
4.3.2	Process issues: • Non-serial-numbered transactions or out-of-sequence invoices or other documents • Duplicate invoices • Creation of fictitious accounts, transactions, employees, charges • Payroll checks with unusual/questionable endorsements • Payees have similar names/addresses • Non-payroll cheques written to an employee • Excessive journal entries • Use of several different banks, or frequent bank changes; use of several different bank accounts • Transfers to or via any type of holding or suspension account		
4.3.3	Deviation from standard procedures (all files but one handled a particular way; all documents but one included in file, etc.)		

4.3.4	Inter-fund loans to other linked organisations		
4.3.5	Failure to disclose unusual accounting practices or transactions		
4.3.6	Defining delivery needs in ways that can only be met by one source		
4.3.7	Continued reliance on person/entity despite poor performance		
4.3.8	Materials erroneously reported as purchased; repeated purchases of same items; identical items purchased in different quantities within a short time period; equipment not used as promised, doesn't work, doesn't exist		
4.3.9	Charging items to project account for personal purposes (books and supplies bought for family members, home gym equipment charged to project account etc.)		

5	**Other**		
	Personal behaviours: • Uncharacteristic willingness to settle questioned costs • Eagerness to work unusual hours • Access to/use of computers at unusual hours • Reluctance to take leave • Insistence on doing job alone • Refusal of promotion or reluctance to change job		
6	**Potential methods for concealing fraud**		
6.1	During an audit or when verifying transactions for approval the auditee may demonstrate some of the following behaviours: • Refusal or reluctance to turn over documents • Unreasonable explanations • Annoyance at questions • Trying to control the audit process (timetables, access, scope) • Auditee blames a mistake on a lack of experience with financial requirements or regulations governing funding • Promises of cooperation followed by subsequent excuses to limit or truncate co-operation • Subtle resistance • Answering a question that wasn't asked • Offering more information than asked • Providing wealth of information in some areas, little to none in others • Explaining a problem by saying "we've always done it that way", or "someone at DfE (or elsewhere) told us to do it that way" or "Mr X said he'd take care of it" • A tendency to avoid personal responsibility (overuse of "we" and "our" rather than "I"); blaming someone else • Too much forgetfulness • Trying to rush the audit process		
6.2	Digital Concealment: Use of "spoofed" email addresses that look like senior leaders; deletion of		

	audit logs in accounting software; or refusal to allow IT audits of remote-access logs.		
6.3	Social Engineering: Using "urgency" or "secrecy" (e.g., "The CEO needs this paid now for a confidential merger") to bypass standard controls		