

## **Anti-Fraud Policy**

### **1. Introduction**

The Anti-Fraud Policy outlines The LSBU Group's position on fraud and sets out responsibilities for its prevention and detection. The policy is intended to ensure that all cases of suspected fraud are promptly reported, investigated and dealt with as necessary, thereby safeguarding the finances and resources of the University and its subsidiaries.

It applies to all staff and students in within the LSBU Group – i.e. London South Bank University, South Bank Colleges, South Bank Academies and any subsidiary companies.

### **2. Relevant Legal Acts and requirements**

The **Fraud Act 2006** legislation defines the offense of fraud in the UK and outlines the various ways in which fraud can be committed. It covers fraudulent activities such as false representation, failure to disclose information, and abuse of position.

The **Economic Crime and Corporate Transparency Act 2023** has introduced a 'failure to prevent fraud' offence, intended to hold organisations to account if they profit from fraud committed by their employees or agents. The Act also broadens the 'identification doctrine' for criminal liability an organisation could be held criminally responsible for, widening the scope from, typically, Directors and Governors to now include actions by a 'senior manager' where they commit a 'relevant offence' such as bribery, money laundering, fraud, false accounting, fraudulent trading and other similar crimes.

This Anti-Fraud Policy, including our zero-tolerance statement on fraud and the related response plan are part of our defence against the risk of suffering a 'failure to prevent' offence associated with a case of fraud.

### **3. Policy**

**The LSBU Group has a clear zero tolerance stance on fraud in any form. We aim to prosecute anyone who commits fraud against the University, Colleges or Schools.**

Consistent with our values and behavioural framework, the Group requires all staff and students to act honestly, with integrity and to safeguard any Group resources for which they are responsible at all times.

Holders of letters of delegated authority are formally responsible for ensuring that all staff are aware of the Group's fraud reporting protocols and that all incidents of suspected theft, fraud, misuse of the Group's assets or serious weaknesses in internal control are reported in accordance with the procedures set out in this document.

#### **4. Definition of fraud**

Fraud can be defined as the use of deception with the intention of:

- Gaining an advantage, personally and/or for family or friends
- Avoiding an obligation

Causing a financial loss to the University or any subsidiary or associated company. Whilst not a definitive list, the main types of fraud are:

- The theft of cash, assets or any other property of the Group by staff or students
- False accounting – dishonestly destroying, defacing, concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with the intent to cause loss to the Group or furnishing information, which is or may be misleading, false or deceptive
- Deliberate claiming of expenses that were not incurred on Group business, or the use of Purchasing Cards for the same purpose
- Abuse of position – abusing authority and misusing resources or information for personal gain or causing loss to the Group
- Entering unfavourable contracts or arrangements with suppliers to benefit personally from the relationship.
- Attempting to make payments to a Group Company with a stolen or unauthorised credit/debit card.
- Money laundering (covered by the Group's Anti Money Laundering Policy)
- Insurance Fraud
- Bribery (Covered by the Group's Anti Bribery Policy)
- Cyber fraud

#### **5. Prevention of fraud**

Fraud is costly, both in terms of reputational risk and financial loss, as well as time consuming to identify and investigate. Therefore, minimising the risk of fraud is a key objective.

The University Group has established systems and procedures in place which incorporate effective and efficient internal financial controls. One of the main objectives of these controls is to minimise the risk of fraud and allow fraud to be detected promptly. These systems and processes are embodied in Financial Regulations, and it is therefore important that all staff are aware of, and follow, Financial Regulations.

All staff should be vigilant and consider the risk of fraud within their areas. Staff should notify their line manager if they believe an opportunity for fraud exists because of poor procedures or lack of effective supervision. The Finance Department can provide guidance where procedures need to be improved.

Managers should be aware that certain patterns of behaviour may indicate a desire for concealment, including:

- Taking few holidays
- Resistance to delegation
- Resentment to normal discussion of work issues
- Frequently working late or at weekends without an obvious reason or outside of agreed work patterns.

With many staff now working flexibly or from home, patterns of leave, working alone or outside of normal business hours are often part of normal working arrangements, but managers should still consider the risk of fraud when the reasons for these patterns of behaviour are not understood.

EFSA has published indicators of potential fraud: education providers, which provides information for academies, colleges, private training providers and employer providers in receipt of the ESFA funding to help them identify potential fraud.

<https://www.gov.uk/government/publications/post-16-audit-code-of-practice/post-16-audit-code-of-practice-2020-to-2021-web-accessible-version#annexd>

## **Reporting a suspected fraud**

Any member of staff who suspects that fraud has been committed must report the matter immediately to their line manager. The line manager should then immediately inform their head of department who will share this information with the Group Chief Financial Officer. Staff should not delay reporting while they investigate or build up a case themselves.

The LSBU Group has a Speak Up hot line which may be used by staff who, for any reason, wish to submit information outside of the management chain described above.

Staff are encouraged to speak up as soon as possible. The policy can be viewed on the staff intranet. All reported cases of suspected fraud will be investigated.

The internal and external auditors have their own procedures for reporting any incidences of suspected fraud that they discover during the course of their audit work however any material fraud identified outside of these processes where LSBU group is a victim, will be reported to the external auditors as soon as possible and the relevant governance committee as soon as possible.

## **6. Fraud Response plan**

When an incidence of fraud is identified, there is an immediate need to safeguard assets, recover losses and secure evidence for legal and disciplinary processes. In order to meet these objectives, the Group has a fraud response plan. Staff and students are required to act in accordance with the fraud response plan.

If a member of staff discovers or suspects a fraud, theft, corruption or other financial irregularity, they must immediately inform their line manager. The line manager will immediately inform the head of department or Dean who will share the information with the Group Chief Financial Officer. In SBC the line manager will share it with the relevant Head of Department and the Executive Principal and Vice Principal Finance & Performance before sharing with the Group CFO. In SBA the line manager should share with the relevant Head of Department who will share with the School Principal and Vice Principal Finance & Performance before sharing with the Group CFO. Failure to report suspected fraud will result in disciplinary action. The Group Chief Financial Officer will instigate the following responses:

- Take action to mitigate the potential loss to the University Group
- Immediately inform the Vice Chancellor, the Group Secretary, the Internal Audit Service and, where appropriate, the Group's Employee and Officers insurers.
- As soon as practical, inform the Chair of the Group Audit and Risk Committee, and, if it involves SBA or SBC, the Chair of the relevant SBA or the SBC Audit Committee.
- Initiate an investigation. The scope of this investigation should be agreed with the Vice Chancellor and the Group Secretary.
- For incidents occurring in SBC or SBA the Group Chief Financial Officer will inform The College and School Executive Principal and College and Trust CFO so that they can assist with actions to mitigate losses and with the investigation.
- Decide whether or not to treat this incident as a criminal investigation and involve the police and/or accredited fraud investigators
- Take steps to prevent a recurrence of such an irregularity or breach of internal controls.

**If it is suspected that a fraud may be significant:**

- The chair of the Group Audit and Risk Committee, the Chair of the Board of Governors and the University, College or Trust Accounting Officer should also be informed. The Chair of the Group Audit and Risk Committee will decide whether or not to convene an extraordinary meeting of The Group Audit and Risk Committee to consider action already taken or proposed to be taken.
- The Group CFO will liaise with the VC, Chairs of Audit Committees and Head of Internal Audit as appropriate to determine the role of internal audit in the investigation.
- The OfS when the matter occurring in the University constitutes a reportable event.

(The Accountability and Audit: OfS Code of Practice, which flows from the OfS Financial Memorandum, contains a mandatory requirement that any significant fraud must be reported to the OfS Accounting Officer)

The Group CFO, Vice Chancellor and Group Secretary will decide whether a suspected fraud is significant (unless one of them is suspected of being involved, but generally a fraud is significant if any of the following apply:

- The sums of money involved are significant
- The fraud involves senior officers of the University or Group
- The particulars of the fraud or irregularity are novel, unusual or complex
- There is likely to be public interest because of the nature of the fraud or irregularity, or the people involved.
- Any fraud relating to the misuse of public funds
- Any other financial fraud where the value is deemed to be significant.

The Accounting Officer of SBC is required to disclose in the annual Statement of Regularity, Propriety and Compliance fraud due to it being 'irregular and improper.'

In the event of a suspected fraud involving a member of the Finance Department in any Group Entity, the Vice Chancellor will initiate action, and The Group Chief Financial Officer will not be involved in the subsequent investigations nor will any member of staff in any of the group Finance teams.

In the event of a suspected fraud involving the Vice Chancellor, the Group Chief Financial Officer will inform the Chair of the Board of Governors directly. Similarly, in the event of a suspected fraud involving the Executive Principal or College CFO, or Trust Business Manager, the Group Chief Financial Officer will inform the chair of the SBC or SBA board directly.

## **Investigation of a suspected fraud**

The investigation must be conducted on a timely basis, in line with University Group procedures and preserving confidentiality.

All staff must cooperate in an investigation or action to mitigate loss and must observe reasonable expectations of confidentiality.

The Vice Chancellor or the Head of Institution for SBC or SBA, may take action during the investigation against any member of staff who is potentially implicated in the suspected fraud. This action may include:

- Temporary suspension from duty
- Denial of access to University Group buildings and computer networks

## **Result of investigation**

If an allegation is substantiated, the action taken by the Vice Chancellor as a consequence will be recorded in writing. Such action should be proportionate to the allegation but may include:

- Temporary suspension from duty
- Denial of access to University Group buildings and computer networks
- Summary dismissal or dismissal under notice
- Notification of the police
- Notification of other parties likely to be affected
- Restitution by the perpetrator
- Other disciplinary procedures