

The American School in London

Anti-Fraud Policy

The current version of any policy, procedure, protocol or guideline is the version posted on the ASL website. It is the responsibility of all employees to ensure that they are following the most up-to-date version.

Responsible party	Director of Finance and Operations
Approved by	Admin Finance Committee
Approval date	May 2026

1. Introduction

The School is committed to the prevention of fraud and the promotion of an anti-fraud culture. It adopts a zero-tolerance attitude to fraud and requires all individuals to act honestly and with integrity at all times, and to report all reasonable suspicions of fraud.

Fraud may occur internally or externally and may be perpetrated by employees, consultants, suppliers or contractors, acting alone or in collusion with others.

The School will investigate all instances of actual, attempted and suspected fraud committed by employees, consultants, suppliers and other third parties and will seek to recover funds and assets lost. Perpetrators will be subject to disciplinary and/or legal action.

This policy sets out responsibilities for fraud prevention, what to do if fraud is suspected and how the school will respond.

2. Regulatory Framework

The School operates within a UK legal and regulatory framework that requires it to take reasonable steps to prevent, detect, and respond to fraud.

Key legislation and guidance include:

- Fraud Act 2006

- Economic Crime and Corporate Transparency Act 2023
- Public Interest Disclosure Act 1998

As a registered charity, the School is also expected to comply with guidance issued by the Charity Commission for England and Wales, including requirements to report serious incidents where appropriate.

This policy forms part of the School's wider framework of governance, risk management, and internal control.

3. Scope

This policy applies to all individuals working for the School at all levels, including employees (permanent, fixed-term and temporary), trustees, volunteers, consultants, contractors and agents.

4. Definition of fraud

Fraud is the use of deception to gain an advantage or cause loss to another party. It may include theft, misuse of funds or resources, false accounting, or the provision of false or misleading information.

Individuals may be prosecuted under the Fraud Act 2006, including where they:

- Make a false representation
- Fail to disclose information where there is a legal duty to do so
- Abuse a position of trust

5. Fraud Risk Assessment

The School adopts a risk-based approach to fraud prevention.

A fraud risk assessment will be conducted at least every 2 years to identify and evaluate the key fraud risks facing the School, taking into account changes in operations, systems, and the external environment.

The assessment will:

- Identify areas of higher fraud risk (e.g. income collection, procurement, payroll, and cyber-enabled fraud)
- Evaluate the effectiveness of existing controls
- Identify control gaps and required improvements

The assessment is facilitated by the Director of Finance and Operations and reported to the Admin Finance Committee, with actions implemented as appropriate.

6. Fraud Prevention and Internal Controls

The School maintains systems of internal control designed to mitigate the fraud risks identified through its risk assessment process. These controls are regularly reviewed and strengthened where necessary.

Key elements of the School's control environment include:

A. Financial controls

- Segregation of duties and dual authorisation requirements for financial transactions, including payments
- Clearly defined approval limits and oversight of expenditure
- Use of a modern accounting system with appropriate user access controls, audit logs, and automated reconciliation processes

B. Procurement and supplier management

- Competitive tendering processes for major contracts
- Periodic review and rotation of suppliers where appropriate
- Verification of supplier details, including independent validation of bank account changes

C. Payroll and HR controls

- Pre-employment checks, including DBS checks and verification of qualifications where relevant
- Transparent and controlled payroll processes, including appropriate review and approval procedures

D. Cyber security and systems controls

- A comprehensive cyber security framework, including multi-factor authentication, anti-malware protections, and periodic penetration testing
- Monitoring of system access and activity to detect unusual or unauthorised behaviour

E. Culture, awareness and reporting

- Clear communication of the School's anti-fraud and whistleblowing policies to all staff
- Encouragement of a culture of openness, accountability, and prompt reporting of concerns

These controls are supported by ongoing monitoring and periodic review to ensure they remain effective in addressing evolving fraud risks.

7. Responsibilities

The Director of Finance and Operations is responsible for:

- Developing, implementing and maintaining effective systems of internal control to prevent and detect fraud.
- Conducting the annual fraud risk assessment and reporting the results.
- Ensuring this policy remains up to date and effective.
- Overseeing investigations into suspected fraud, in conjunction with Human Resources, where appropriate.

Trustees are responsible for:

- Safeguarding the assets of the charitable company.
- Taking reasonable steps for the prevention and detection of fraud and other irregularities.
- Determining whether incidents should be reported to the Charity Commission for England and Wales

Managers are responsible for:

- Understanding the fraud risks relevant to their areas
- Ensuring compliance with internal controls and procedures

- Escalating any concerns promptly

Employees are responsible for:

- Acting with integrity and safeguarding the School's assets
- Reporting suspected fraud promptly
- Assisting with investigations where required

8. Cyber and Social Engineering Fraud Risks

The School recognises the increasing risk of fraud occurring through digital and communication channels, including cyber-enabled and social engineering attacks.

Examples include:

- Phishing emails and fraudulent communications
- Business email compromise (e.g. impersonation of senior staff or trustees)
- Supplier bank detail change scams
- Payroll diversion fraud
- Fraudulent fee payment instructions
- Telephone-based fraud (e.g. individuals impersonating suppliers, banks, or staff to request urgent payments or sensitive information)

Employees must:

- Verify any changes to bank or payment details using an independent and trusted method (e.g. known contact details, not those provided in the request)
- Exercise caution with urgent or unusual requests, particularly those involving payments or confidential information
- Not rely solely on email or telephone instructions for financial transactions
- Be alert to impersonation attempts and social engineering tactics
- Report suspicious communications (including emails and phone calls) promptly to the Technology team or Finance team

No payment instructions or changes to supplier or payroll details should be actioned solely on the basis of a telephone request without independent verification.

This section should be read in conjunction with the School's ICT Responsible Use Agreements.

9. Reporting suspicions

All individuals must report suspected fraud promptly and in good faith.

Reports should be made to:

- A line manager, or
- The Director of Finance and Operations, or
- Through the School's Whistleblowing Policy

Concerns will be treated seriously and, where possible, handled confidentially.

The Public Interest Disclosure Act 1998 protects individuals who raise concerns in good faith. Independent advice is available from [Protect](#) (whistleblowing charity).

10. Response to Suspected or Confirmed Fraud

Where fraud is suspected or identified, the School will take a structured and proportionate response.

A. Immediate actions may include:

- Securing assets and preventing further loss
- Suspending relevant transactions or system access
- Preserving evidence (e.g. financial records, emails, devices)
- Maintaining confidentiality

B. Investigation:

- Led by the Director of Finance and Operations, with HR involvement where appropriate
- External specialists (e.g. legal advisers or forensic accountants) may be engaged
- Investigations will be conducted fairly and confidentially

C. Escalation and reporting:

- The Head of School and Chair of the Admin Finance Committee will be informed
- Trustees will be notified as appropriate
- The School will consider:
 - Notifying its cyber insurance provider immediately where there is a possibility of a claim
 - Reporting the incident to the Admin Finance Committee at the next scheduled meeting (or sooner if appropriate)
 - Reporting significant incidents to [Report Fraud](#) (UK's national reporting centre for fraud and cybercrime) - there is no statutory requirement for this but it is helpful for insurance purposes and helping to prevent future instances of fraud
 - Reporting significant incidents to the Charity Commission for England and Wales as a Serious Incident (The Charity Commission expects prompt reporting of fraud, theft or cybercrime where it is significant enough to affect the School's operations, finances or reputation.)

D. Outcomes:

- Disciplinary action, up to and including dismissal
- Referral to law enforcement where appropriate
- Recovery of losses where possible

E. Post-incident review:

Following any fraud incident, the School will conduct a review to identify control weaknesses and implement improvements.

11. Related Policies

This policy should be read in conjunction with:

- Whistleblowing Policy
- ICT Responsible Use Agreements