EDA COLLEGE

EDUCATE I DEVELOP I ACHIEVE

ANTI-MONEY LAUNDERING AND FRAUD PREVENTION POLICY[1]

Version Control/History

Policy Title	Anti-Money Laundering and Fraud Prevention Policy
Policy Reference	EDA-POL-AML-001
Version	1.1
Status	Approved
Approved by	Academic Board
Date of Approval	August 2025
Review Date	August 2026
Approval Date	11 September 2026
Next Review Date	September 2027
Policy Owner	Principal/CEO
Policy Custodian	Finance Lead
Money Laundering Reporting Officer (MLRO)	Finance Lead & Operations Manager
Applies To	All staff, governors, contractors and volunteers

[1] *In accordance with the Proceeds of Crime Act 2002, the Terrorism Act 2000, the Bribery Act 2010, and HMRC / NCA guidance.*

Contents

1. Introduction and Purpose

EDA College Ltd (“the College”) is committed to operating with the highest standards of financial integrity and to protecting itself, its students, its staff and the public from financial crime. Financial crime — including money laundering, fraud, bribery, corruption and the facilitation of tax evasion — is a serious criminal matter that can cause significant harm to individuals, to public institutions and to society as a whole.

This Anti-Money Laundering and Fraud Prevention Policy (“the Policy”) sets out EDA College’s legal obligations, institutional controls and reporting arrangements in relation to money laundering, fraud and related financial crimes. It applies to all staff, governors, contractors and volunteers and compliance is mandatory. Breaches of this Policy may constitute criminal offences and will result in disciplinary action up to and including dismissal.

EDA College recognises that, as a higher education institution handling public funds (student loan income), fee income, and potentially grant and donation income, it is subject to financial crime risks that must be actively managed. This Policy establishes the framework for doing so.

> “EDA College has zero tolerance for money laundering, fraud, bribery and corruption. Every member of our community has a responsibility to act with integrity and to report concerns promptly. Financial crime is not a victimless offence — it harms students, staff and the communities we serve.”

2. Legislative and Regulatory Framework

Legislation / Regulation	Key Requirement Relevant to EDA College
Proceeds of Crime Act 2002 (POCA 2002)	The primary money laundering legislation in the UK; creates three principal offences: laundering (s.327), arranging (s.328) and acquisition/use/possession (s.329); also creates the offence of failing to disclose knowledge or suspicion of money laundering (s.330) and tipping off (s.333A)
Terrorism Act 2000 (TA 2000)	Creates offences of providing or receiving terrorist financing; EDA College must not knowingly handle funds connected to terrorism
Bribery Act 2010	Creates offences of bribing and being bribed; requires organisations with commercial operations to have ‘adequate procedures’ to prevent bribery; applies to EDA College as an organisation with commercial activities (tuition fee income)
Criminal Finances Act 2017	Creates the corporate offence of facilitating tax evasion; EDA College must have reasonable prevention procedures; also strengthens powers relating to unexplained wealth and money laundering
Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (as amended)	Implements EU AMLD requirements in UK law; sets out requirements for customer due diligence, risk assessment and reporting; applies to businesses in regulated sectors
Fraud Act 2006	Creates offences of fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position; applies to both internal and external fraud affecting EDA College
Computer Misuse Act 1990	Criminalises unauthorised access to computer systems; relevant to cyber fraud and hacking directed at EDA College
Modern Slavery Act 2015	Creates offences of slavery, servitude and human trafficking; relevant to identifying vulnerable students who may be connected to organised crime; requires transparency statement from larger organisations
NCA Guidance and HMRC guidance	Non-statutory guidance on reporting suspicious activity; EDA College staff should be familiar with the HMRC guidance for educational institutions and NCA guidance on submitting SARs

3. Scope and Application

This Policy applies to:

- All members of staff employed by EDA College, on any type of contract
- All governors and committee members
- All contractors, agency workers, consultants and volunteers working on behalf of the College
- All financial transactions and financial arrangements involving EDA College, including income from students, grants, donations, employer partnerships and any other source
- All third-party relationships, including suppliers, agents, professional advisors and banking relationships

Compliance with this Policy is mandatory. Any member of staff who fails to comply, who participates in or facilitates money laundering or fraud, or who fails to report a suspicion of money laundering in circumstances where they are legally required to do so, may be committing a criminal offence and will be subject to disciplinary action up to and including immediate dismissal, in addition to any criminal proceedings.

4. Definitions

Term	Definition
Money laundering	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 three stages of money laundering are: Placement (introducing criminal funds into the legitimate financial system); Layering (concealing the trail through complex transactions); Integration (reintroducing funds as apparently legitimate).
Criminal property	Property which constitutes a person's benefit from criminal conduct; it is criminal property regardless of its value and regardless of whether the person committing the offence knows or suspects it to be criminal property (POCA 2002)
Suspicious Activity Report (SAR)	A report submitted to the National Crime Agency (NCA) by the MLRO where there is knowledge or suspicion (or reasonable grounds for knowledge or suspicion) that a person is engaged in money laundering or terrorist financing
Money Laundering Reporting Officer (MLRO)	The designated person at EDA College responsible for receiving internal suspicion reports, assessing them and, where appropriate, submitting SARs to the NCA. At EDA College, the MLRO is the Finance Lead and Operations Manager.
Tipping off	Disclosing to a person who is suspected of money laundering (or to any other person) that a suspicious activity report has been made, or that a money laundering investigation is being considered, in a way that is likely to prejudice any investigation. Tipping off is a criminal offence under POCA 2002 s.333A.
Fraud	A dishonest act carried out with the intention of gaining an advantage or causing loss to another; may be committed by misrepresentation, by failing to disclose information, or by abuse of a position of trust (Fraud Act 2006)
Bribery	Offering, giving, receiving or requesting something of value with the intention of influencing the recipient to act improperly in the exercise of their duties (Bribery Act 2010)
Facilitation of tax evasion	Dishonestly assisting another person in evading their tax obligations; a corporate offence where EDA College fails to prevent an associated person from facilitating tax evasion (Criminal Finances Act 2017)
Politically Exposed Person (PEP)	A person who holds or has held a prominent public function (e.g. head of state, government minister, senior judicial official, senior military officer) and their close associates and family members; PEPs present a higher risk of being involved in bribery and corruption
Nominated Officer / MLRO	Used interchangeably in this Policy; the person responsible for receiving and assessing internal disclosures of suspected money laundering

5. Our Zero-Tolerance Commitments

EDA College adopts a zero-tolerance approach to all forms of financial crime, including money laundering, fraud, bribery, corruption and the facilitation of tax evasion. This means:

- EDA College will not knowingly handle, process or facilitate the movement of funds that represent the proceeds of crime
- EDA College will not engage in or facilitate bribery, corruption or improper payments of any kind
- EDA College will not assist any person in evading their tax obligations
- EDA College will not allow its premises, systems, accounts or reputation to be used to further financial crime
- EDA College will report all suspicions of money laundering or terrorist financing to the MLRO and, where required, to the NCA
- EDA College will report all suspected fraud to the appropriate authorities
- EDA College will investigate all allegations of financial crime involving College funds or staff
- EDA College will not retaliate against or disadvantage any person who reports a genuine financial crime concern in good faith

6. Money Laundering: Understanding the Risk

Money laundering involves three stages, each of which may give rise to criminal liability for EDA College if it is unwittingly involved:

Stage	Description	How It Could Affect EDA College
Placement	Criminal funds are introduced into the legitimate financial system for the first time	Criminals paying tuition fees or making donations with cash or funds from illegitimate sources; bulk cash deposits that do not match the student's apparent circumstances
Layering	The origin of funds is concealed through multiple complex transactions designed to create a confusing audit trail	Requests for refunds of overpaid fees to a different account from the one that paid; complex third-party payment arrangements; unusual payment routes
Integration	The laundered funds are reintegrated into the legitimate economy as apparently clean money	Funds 'recycled' through the College emerging as legitimate tuition fee refunds or grants; funds appearing to flow from legitimate educational activity

EDA College does not operate in one of the sectors where AML regulation is most intensive (such as financial services or legal services). However, it handles significant flows of money — primarily student loan income and direct fee payments — and may be targeted by criminals seeking to exploit these flows. Vigilance is required.

7. EDA College's Exposure to Money Laundering Risk

EDA College has assessed its exposure to money laundering risk across its main activities. The following table summarises the assessed risk areas:

Risk Area	Level	Key Risk	Mitigation
Tuition fee payments from self-funded students	MEDIUM	Cash payments or payments from unknown third-party sources could represent placement of criminal funds	No cash payments over £500 accepted; all payments must be from identified accounts; payment source verification for large or unusual payments
Employer-sponsored students	MEDIUM	Employer sponsors could be fronts for illegitimate businesses seeking to launder funds through educational payments	Written sponsorship agreements required; employer identity verified; Companies House check for new sponsors above threshold

Donations and gifts (where applicable)	MEDIUM-HIGH	Donations from unknown or high-risk sources could represent money laundering	Donor identity to be verified for donations above £1,000; enhanced due diligence for PEPs and high-risk jurisdictions; Board approval for significant donations
Overseas student payments	MEDIUM-HIGH	Payments from high-risk jurisdictions or through unusual intermediary channels	Enhanced scrutiny of payments from high-risk jurisdictions; verification of payment source; no acceptance of payments via unregulated money transfer operators
Grant and funded income	LOW	Generally low risk due to government or institutional source	Standard financial controls; verify grant terms; ensure restricted funds used for designated purpose
Refund requests	MEDIUM	Requests for refunds to a different account from the payer could indicate layering	Refunds only made to the original payment source; any exceptions require Finance Lead approval and MLRO notification
Contractor and supplier payments	LOW-MEDIUM	Payments to shell companies or unusual payment destinations	Supplier due diligence; verified bank details; dual authorisation for large payments

This risk assessment will be reviewed annually by the MLRO and updated to reflect changes in EDA College's activities, new guidance from the NCA or HMRC, and any incidents or near-misses identified during the year.

8. Due Diligence and Know Your Customer

8.1 Standard Due Diligence

EDA College is not a regulated financial institution and is not required to conduct full Know Your Customer (KYC) checks as a matter of routine in the way that banks or solicitors are. However, the College will carry out proportionate due diligence on certain categories of transaction and relationship:

- For self-funded students paying fees in excess of £5,000 per year directly (not through SLC): the student's identity will be verified through the enrolment process (photo ID and address confirmation); the source of large or unusual payments may be queried
- For employer sponsors: the employer's identity will be verified through Companies House or equivalent; a written sponsorship agreement will be required; the employer's legitimacy will be considered if any concerns arise
- For donations and gifts above £1,000: the donor's identity and the source of the funds will be verified before acceptance; donations from anonymous or clearly high-risk sources will not be accepted
- For significant new suppliers and contractors: Companies House or equivalent verification; check that payment details match the company's registered details
- For banking relationships: EDA College will maintain accounts only with UK-regulated banks or building societies

8.2 Enhanced Due Diligence

Enhanced due diligence will be applied in the following circumstances:

- Where a payment comes from or is to be made to a jurisdiction identified by the Financial Action Task Force (FATF) as high-risk or subject to increased monitoring
- Where a proposed donor, sponsor or third-party payer appears to be a Politically Exposed Person (PEP)
- Where any transaction raises a suspicion of money laundering, even at a lower value
- Where a refund is requested to an account different from the original payment source

8.3 Cash Payments

EDA College operates a strict policy on cash payments. Cash creates particular money laundering risks because it is difficult to trace and can easily represent the proceeds of crime.

- EDA College does not accept cash payments for tuition fees
- Cash receipts for other purposes (e.g. petty cash, event proceeds) are subject to the petty cash procedures in the Financial Regulations
- Any unusual or unexpected offer of cash payment must be reported to the MLRO immediately
- Under no circumstances should any member of staff accept cash from a student, applicant, sponsor or external party outside of the College's normal petty cash procedures

9. Suspicious Activity: Recognising the Signs

All staff should be alert to the signs of potential money laundering or financial crime. The following are indicators that should prompt a report to the MLRO. No single indicator is necessarily conclusive — staff should exercise judgement and report any genuine concern:

Category	Red Flag Indicators
Unusual payment behaviour	Payment of tuition fees in cash or by unusual means; payment of fees by a third party with no clear legitimate connection to the student; payment from multiple accounts or in multiple small amounts that appear designed to avoid detection; payment from an account in a different name from the student without satisfactory explanation
Overpayment requests	A student or third party pays significantly more than the amount due and then requests a refund of the difference, particularly to a different account; this is a classic money laundering indicator
Student profile inconsistency	A student's apparent lifestyle, expenditure or behaviour appears inconsistent with the fees or financial support they are receiving; apparent lack of genuine academic interest combined with a strong focus on financial transactions
Identity concerns	Documents provided do not appear genuine; a student provides different identity information at different stages; a student appears to be acting on behalf of or under the control of another person
Geographic or jurisdiction risk	Funds originating from or being sent to a jurisdiction associated with high levels of financial crime or subject to sanctions; use of accounts in unusual jurisdictions without satisfactory explanation
Unusual refund requests	Requests for refunds to an account other than the one from which payment was made; requests for refunds in cash; requests for refunds of amounts not owed; pressure to process refunds quickly without adequate documentation
Structuring	Multiple transactions just below reporting or approval thresholds, suggesting deliberate structuring to avoid scrutiny
Evasiveness or unusual interest	A person who is unduly interested in the College's financial processes, reporting procedures or audit arrangements; a person who is evasive when asked routine questions about a transaction
Sponsor or third-party concerns	An employer sponsor that cannot be readily verified through Companies House or similar; a sponsor whose business appears unrelated to the student's field of study; a sponsor who pays unusually quickly or via unusual channels

> If in doubt, report. You do not need to be certain that money laundering is occurring before making an internal report to the MLRO. The MLRO's role is to assess the concern. A concern raised in good faith that turns out to be unfounded will not have any adverse consequences for the person who raised it.

10. Reporting Suspicious Activity (SARs)

10.1 Internal Reporting

Any member of staff who knows or suspects, or has reasonable grounds to know or suspect, that a person is engaged in money laundering or terrorist financing MUST report their concern to the MLRO as soon as possible. This is a legal obligation under POCA 2002 s.330 for staff who are in the 'regulated sector' (which may include certain EDA College financial activities), and is a policy obligation for all staff.

> Failure to report a suspicion of money laundering when you are legally required to do so is a criminal offence under POCA 2002 s.330, punishable by up to five years' imprisonment. Ignorance of the law is not a defence. If you have a concern, you must report it to the MLRO. Do not investigate it yourself.

To make an internal report:

1. Contact the MLRO (Finance Lead and Operations) immediately by telephone or in person
2. Complete the Internal Suspicious Activity Report Form (Appendix A) as soon as possible after the verbal report
3. Do not discuss your concern with anyone other than the MLRO
4. Do not take any further action on the suspicious transaction until you have spoken to the MLRO
5. Preserve all documents, correspondence and evidence related to the concern

10.2 MLRO Assessment and External Reporting

On receipt of an internal SAR, the MLRO will:

- Assess the concern and gather any additional relevant information
- Decide whether to submit a Suspicious Activity Report to the National Crime Agency (NCA) via the NCA's online reporting system (www.nationalcrimeagency.gov.uk)
- Obtain a 'consent' (Defence Against Money Laundering, DAML) from the NCA before proceeding with a suspicious transaction where required
- Record the decision and the reasons, whether or not a SAR is submitted
- Advise the reporting staff member of the outcome, to the extent that confidentiality permits

10.3 Consent Requests

Where the MLRO concludes that a suspicious transaction has not yet occurred but is about to occur, they will submit a request for consent (a DAML) to the NCA before the transaction proceeds. EDA College will not proceed with a suspicious transaction while awaiting consent from the NCA, unless the NCA consents or the moratorium period expires without a response.

11. The Money Laundering Reporting Officer (MLRO)

EDA College's Money Laundering Reporting Officer (MLRO) is the Finance Lead and Operations Manager. The MLRO is responsible for:

- Receiving all internal disclosures of suspected money laundering or terrorist financing
- Assessing each internal disclosure and deciding whether to submit a SAR to the NCA
- Submitting SARs to the NCA where required
- Maintaining a record of all internal disclosures, MLRO assessments and SAR submissions
- Maintaining and reviewing the College's AML risk assessment annually
- Providing AML training to staff
- Advising the Principal / CEO and the Board on AML compliance
- Liaising with the NCA, HMRC and other relevant agencies on AML matters

In the absence of the MLRO, reports should be made to the Principal / CEO, who will act as deputy MLRO. The MLRO must be contactable at all times when the College is operating. The MLRO's contact details are published internally and are set out in Appendix D.

> The MLRO acts independently in fulfilling their AML duties. No other member of staff or governor, including the Principal / CEO, may direct the MLRO not to submit a SAR to the NCA where the MLRO

has assessed that submission is required. Any attempt to pressure the MLRO in this way must itself be reported to the NCA.

12. Tipping Off and Confidentiality

Tipping off is one of the most serious obligations in UK money laundering law. It is a criminal offence under POCA 2002 s.333A to disclose to a person who is suspected of money laundering — or to any third party — that a suspicious activity report has been made, or that an investigation is being considered, where this disclosure is likely to prejudice any investigation.

DO NOT tell the person you suspect, or anyone else (other than the MLRO), that you have made or are considering making a report. Do not ask the suspected person to explain their conduct, as this could constitute tipping off. If the suspected person asks why a transaction is being delayed, refer them to the MLRO and do not provide any explanation yourself.

Permitted disclosures include:

- Disclosures to the MLRO as part of the internal reporting process
- Disclosures to a legal advisor for the purpose of obtaining legal advice
- Disclosures to law enforcement agencies in connection with an investigation
- Disclosures to the OfS or other regulators in fulfilment of regulatory obligations

If a staff member is approached by a suspected person who appears to have become aware of a SAR, the staff member should immediately contact the MLRO and avoid confirming or denying any information.

13. Fraud Prevention

EDA College is committed to preventing all forms of fraud, both by protecting itself from external fraud and by preventing internal fraud by its own staff. Fraud causes direct financial loss to the College, diverts resources from students, and undermines institutional trust.

EDA College’s approach to fraud prevention is based on four pillars: PREVENT (reducing the opportunity for fraud through strong controls); DETECT (identifying fraud quickly when it does occur); RESPOND (investigating and taking action swiftly and proportionately); LEARN (improving controls based on incidents and near-misses).

14. Types of Fraud Relevant to EDA College

Fraud Type	Description	Typical Perpetrator
Payroll fraud	Adding fictitious employees to payroll; inflating salaries; submitting false overtime or expense claims	Internal (staff)
Procurement fraud	Accepting bribes or kickbacks from suppliers; creating fictitious suppliers; colluding with suppliers on pricing	Internal (staff) or external-internal collusion
Grant fraud	Misusing grant funds; submitting false grant claims; fabricating research data or activity reports	Internal (staff) or student
Expense fraud	Submitting false or inflated expense claims; claiming for personal items; creating fictitious receipts	Internal (staff or governors)
Student finance fraud	Students submitting false information to Student Finance England to obtain loans they are not entitled to; ‘ghost students’ — enrollment of fictitious students to generate SLC income for the College	Student; internal-external collusion (very serious)
Identity fraud	Applicants or students using false identity documents to gain admission or access student finance	External (applicants / students)
Invoice fraud / mandate fraud	Fraudulent invoices submitted by external parties; criminals impersonating suppliers and requesting bank detail changes	External

Cyber fraud / phishing	Email-based fraud targeting staff to extract financial information or authorise fraudulent payments; ransomware; account takeover	External
Asset misappropriation	Theft or misuse of College physical or intellectual assets; unauthorised use of College facilities	Internal (staff) or external
Admissions fraud	Forged qualification documents; paid essay writing (contract cheating) presented as the student's own work	External (applicants); student

15. Fraud Risk Controls

EDA College's primary fraud controls are set out in the Financial Regulations. The following summarises the key controls relevant to fraud prevention:

Control	How It Prevents Fraud
Segregation of duties	No single person can initiate, approve and record a financial transaction; prevents individual fraud without collusion
Dual authorisation for payments above £2,000	Two authorised signatories required for all significant payments; prevents individual payroll or payment fraud
Purchase order system	All purchases above £100 require a pre-approved purchase order; prevents fictitious supplier payments and unauthorised commitments
Supplier due diligence and bank detail verification	All new suppliers verified through Companies House; bank details verified before first payment and not changed without dual verification; prevents mandate fraud
Payroll reconciliation to HR establishment	Monthly reconciliation of payroll to the approved list of posts and salaries; prevents fictitious employee fraud
Regular management accounts	Monthly financial reports reviewed by the Principal / CEO; financial anomalies visible and challenged; reduces the window for undetected fraud
Bank reconciliation	Monthly bank reconciliations signed off by the Principal / CEO; prevents misposting and concealment of fraudulent payments
External audit	Annual audit by an independent external auditor; provides independent assurance on financial controls
Expense claim approval	All expenses approved by the claimant's line manager; Principal's expenses approved by the Board Chair; receipts required; prevents expense fraud
Access controls for financial systems	Role-based access to financial systems; access removed promptly on leaving; audit logs maintained; prevents unauthorised transaction processing
Whistleblowing channels	Clear, protected routes for staff to report suspected fraud without fear of reprisal; increases the probability of detection

16. Internal Fraud by Staff

EDA College recognises that internal fraud — fraud committed by its own staff, governors or contractors — is one of the most significant fraud risks it faces. Internal fraudsters exploit their trusted position and knowledge of internal controls to commit fraud in ways that are harder to detect than external fraud.

16.1 Prevention

- All new staff are subject to pre-employment checks, including reference checks and (where relevant to the role) DBS and credit checks
- Staff with access to financial systems or assets are reminded of their obligations under this Policy at induction and annually
- The College maintains clear expense and purchasing policies and actively monitors compliance

- An anonymous internal reporting channel is available (see Section 22)
- The College conducts unannounced spot checks on petty cash and other cash-handling processes

16.2 Detection

- Monthly management accounts are reviewed by the Principal / CEO; anomalies are investigated promptly
- The external auditor conducts sampling of transactions during the annual audit
- All significant or unusual transactions are subject to dual authorisation and management review
- The payroll is reconciled to the HR establishment monthly

16.3 Response to Internal Fraud

Where internal fraud by a member of staff is suspected:

- The matter will be reported to the Principal / CEO (or to the Chair of the Board if the Principal is involved) immediately
- The Finance Lead will take immediate steps to preserve evidence and to prevent further loss (e.g. suspending access to financial systems)
- The member of staff will be suspended pending investigation, in accordance with the College's HR procedures
- The matter will be investigated in accordance with the Disciplinary Procedure, using an independent investigator where appropriate
- Where the evidence supports it, the matter will be referred to the police for criminal investigation
- Civil recovery of assets will be considered in consultation with legal advisors
- All internal fraud incidents, however minor, will be reported to the Finance Board and, where material, to the Board of Governors

17. External Fraud

EDA College is also at risk of fraud perpetrated by external parties, including applicants, students, suppliers and criminals who have no prior relationship with the College.

17.1 Student Finance Fraud

One of the most serious external fraud risks for EDA College is student finance fraud, including:

- 'Ghost student' fraud: where individuals claim to be enrolled students and obtain SLC funding to which they are not entitled, potentially with internal collusion
- False identity documents used to gain admission and access SLC funding
- Students providing false information to SFE about their circumstances to obtain higher maintenance loans

EDA College's controls against student finance fraud include:

- Robust identity verification at enrolment (photo ID and address proof)
- Regular attendance monitoring and SLC reporting reconciliation
- Any discrepancy between enrolled student numbers and SLC funding claims is investigated immediately by the Finance Lead
- All concerns about student finance fraud are reported to the SLC Fraud Reporting Service

17.2 Mandate Fraud / Invoice Fraud

Mandate fraud (also known as bank detail change fraud) involves criminals contacting EDA College and impersonating a known supplier or bank, requesting a change of payment details, so that future payments are redirected to the criminal's account.

- EDA College will never change a supplier's bank details based solely on an email, letter or telephone request
- Any request to change bank details must be verified by telephone to the supplier's known number (not the number given in the request) before the change is made in the financial system

- The verification call and its outcome must be documented and signed by the Finance Lead before any payment is made to the new details

18. Cyber Fraud and Phishing

Cyber fraud, including email phishing, business email compromise and ransomware, represents a growing and significant threat to organisations of all types, including higher education institutions. EDA College is committed to maintaining robust cyber security defences and to training staff to recognise and resist cyber fraud.

18.1 Key Cyber Fraud Risks

- Phishing emails designed to steal login credentials or direct staff to fraudulent websites
- Business email compromise: criminals impersonating the Principal / CEO or Finance Lead by email, requesting urgent wire transfers or changes to payment details
- Ransomware attacks that encrypt College data and demand payment
- Fraudulent invoices sent by email that appear to be from known suppliers
- Credential theft targeting College email or financial system accounts

18.2 Staff Responsibilities

- Staff must never click on links or attachments in emails that appear suspicious, unexpected or from unknown senders
- Staff must never provide their login credentials, passwords or financial authorisation codes in response to an email request
- Staff must never process a payment or change bank details based solely on an email instruction from a senior colleague without independent verification; legitimate urgent payment requests will always be verifiable by an alternative means
- Any suspected phishing email or cyber incident must be reported to the IT Manager immediately
- Staff should not use personal email for College business and should not access College systems from public or unsecured Wi-Fi without a VPN

> EDA College will NEVER instruct staff to make payments, change bank details or provide sensitive information via email alone, without an additional verification step. If you receive an email instruction of this nature that feels unusual, even from someone who appears to be a senior colleague, call them on a known number to verify before acting.

19. Bribery and Corruption

EDA College is committed to conducting all its activities with complete integrity and in compliance with the Bribery Act 2010. Bribery is the offering, giving, receiving or requesting of any financial or other advantage with the intention of improperly influencing a decision or action. EDA College has zero tolerance for bribery, whether by its staff, governors, agents or on its behalf by any third party.

19.1 Prohibited Conduct

- No member of staff or governor may offer, give, request or accept a bribe in any circumstances
- No member of staff may make or receive any payment that is not properly authorised and recorded in EDA College's financial systems
- No member of staff may use their position at EDA College to obtain personal advantage by improper means
- No agent, partner or third party may offer or give a bribe on behalf of EDA College or in connection with EDA College's business

19.2 Gifts and Hospitality

Gifts and hospitality from third parties (suppliers, contractors, professional advisors, potential partners) present a particular bribery risk. EDA College's gifts and hospitality policy is:

- Staff may accept gifts of modest value (below £50) from known and legitimate business contacts in circumstances where this is reasonable and customary, provided the gift is declared to the Finance Lead and recorded in the Gifts Register
- No member of staff may accept cash gifts, gifts of significant value (above £50), or gifts that are conditional on the recipient acting in a particular way
- No member of staff may accept gifts or hospitality from a supplier or contractor while a procurement process in which that supplier or contractor is participating is ongoing
- EDA College staff may offer modest and proportionate hospitality to external parties in the course of legitimate business, subject to the Finance Lead's approval for amounts above £100 per person
- All gifts received and hospitality given or received above £25 must be recorded in the Gifts and Hospitality Register maintained by the Finance Lead.

19.3 Facilitation Payments

Facilitation payments are unofficial payments made to government officials or others to secure or expedite the performance of a routine function they are otherwise required to perform. Facilitation payments are illegal under the Bribery Act 2010 regardless of their amount, the jurisdiction in which they are made, or the local practice. EDA College staff must not make facilitation payments under any circumstances.

20. Facilitation of Tax Evasion

The Criminal Finances Act 2017 created a new corporate offence of failing to prevent the facilitation of tax evasion by an 'associated person' (a member of staff, agent or contractor) of the College. This means EDA College could be criminally liable if a member of staff or agent dishonestly facilitates tax evasion by a third party, even if the College itself had no knowledge of it.

20.1 What Counts as Facilitation

The corporate offence may be committed where an associated person:

- Assists a student, employer or other person to evade tax by, for example, providing false invoices, falsifying records, or providing misleading information to HMRC
- Allows the College to be used as a vehicle to provide fraudulent tax deductions (e.g. false training cost invoices)
- Accepts cash payments in a way designed to help a payer conceal income from HMRC

20.2 Prevention Measures

- All financial transactions must be properly documented, authorised and recorded; no off-book payments are permitted
- All invoices issued by EDA College must accurately reflect the services provided
- No member of staff may assist any person (including students, employers or suppliers) in evading tax
- Any request that appears designed to facilitate tax evasion must be refused and reported to the MLRO
- EDA College's payroll will be operated in full compliance with HMRC PAYE requirements; no cash-in-hand payments are permitted

21. Modern Slavery and Financial Crime

EDA College recognises that modern slavery and human trafficking are serious crimes that may intersect with money laundering and fraud. Students who are victims of modern slavery may have their financial affairs controlled by exploiters, and the proceeds of modern slavery may be laundered through educational institutions.

- Staff should be alert to signs that a student's financial arrangements appear to be controlled by another person (e.g. all financial transactions controlled by a third party; the student appears to have no independent access to their own funds; the student appears fearful or under coercion)
- Where modern slavery is suspected in connection with a student, the concern must be reported to the Designated Safeguarding Lead AND to the MLRO
- EDA College will refer all modern slavery concerns to the National Referral Mechanism (NRM) and, where appropriate, to the police

- For organisations of a certain size, EDA College will publish a Modern Slavery Transparency Statement on its website annually in accordance with the Modern Slavery Act 2015

22. Whistleblowing

EDA College encourages all staff, governors and contractors to report concerns about financial crime, money laundering, fraud, bribery or corruption through the College's whistleblowing procedures. Whistleblowing is a vital tool for detecting financial crime that might otherwise go undetected.

22.1 Internal Reporting Routes

Concern Type	Report To	Alternative If Implicated
Money laundering / terrorist financing suspicion	MLRO (Finance Lead and Operations Manager)	Principal / CEO if MLRO is involved
Internal fraud by a member of staff	Finance Lead; then Principal / CEO	Chair of the Finance Board if Principal is involved
Fraud by the Principal / CEO	Chair of the Board of Governors	Finance Board Chair
Bribery or corruption	Finance Lead; Principal / CEO	Chair of the Finance Board
Facilitation of tax evasion	MLRO (Finance Lead)	Principal / CEO
Any financial crime (general)	MLRO in the first instance	Chair of the Board of Governors if senior staff are involved

22.2 External Reporting Routes

Staff who are not satisfied with the response to an internal report, or who believe the concern involves senior leadership, may report directly to:

- The National Crime Agency (NCA): www.nationalcrimeagency.gov.uk/submit-a-sar (for money laundering suspicions)
- Action Fraud (national fraud reporting centre): 0300 123 2040 | www.actionfraud.police.uk
- HMRC Fraud Hotline: 0800 788 887 (for tax evasion and customs fraud)
- The Office for Students (OfS): where the concern affects OfS regulatory compliance
- The Student Loans Company Fraud Reporting Service (for student finance fraud)

22.3 Protection for Whistleblowers

Staff who report financial crime concerns in good faith are protected by the Public Interest Disclosure Act 1998 (PIDA) and EDA College's Whistleblowing Policy. They will not be subjected to any detriment, disciplinary action or dismissal as a result of making a genuine report. Anonymous reports will be investigated where sufficient information is provided.

23. Investigation and Sanctions

23.1 Investigations

EDA College will investigate all reports of suspected financial crime promptly and thoroughly. Investigations will be led by the Finance Lead in the first instance, with the involvement of external investigators, legal advisors or forensic accountants where the scale or complexity of the concern warrants it. Where a concern involves the Manager of Finance or the Principal / CEO, the investigation will be led by the Chair of the Finance Board with external assistance.

23.2 Preservation of Evidence

From the moment a financial crime concern is raised, EDA College will take steps to preserve all relevant evidence, including:

- Securing access to financial system records, emails and other electronic data

- Securing paper documents and records
- Suspending the relevant financial system access of any staff member under investigation
- Not interfering with or destroying any evidence that may be relevant to a criminal investigation

23.3 Referral to Authorities

EDA College will refer suspected financial crime to the appropriate authorities:

- Money laundering and terrorist financing: MLRO to submit SAR to the NCA
- Fraud: referral to Action Fraud and/or the police
- Tax evasion: referral to HMRC
- Student finance fraud: referral to the Student Loans Company Fraud Team
- Bribery: referral to the police / Serious Fraud Office where appropriate

23.4 Disciplinary Sanctions

Staff who are found to have committed, participated in or facilitated financial crime will be subject to the most serious disciplinary sanctions available, up to and including summary dismissal for gross misconduct. Governors found to have engaged in financial crime will be subject to removal from office. In addition to disciplinary action, EDA College will actively support criminal prosecution and civil recovery of assets where appropriate.

> Financial crime committed by EDA College staff is not only a disciplinary matter — it is a criminal offence. EDA College will not seek to resolve financial crime matters through internal processes alone where criminal conduct is established. We will support police investigations and prosecution.

24. Training and Awareness

Training	Audience	Frequency	Lead
AML and fraud awareness training (mandatory)	All new staff and governors	At induction	MLRO / Finance Lead
Annual AML and fraud refresher	All staff and governors	Annually	MLRO
MLRO-specific AML training	Finance Lead (as MLRO); Deputy MLRO (Principal / CEO)	On appointment; every 2 years or when legislation changes	External provider
Cyber fraud and phishing awareness	All staff	At induction; annually; following any significant cyber incident or threat	IT Lead / MLRO
Bribery Act awareness	All staff who engage with suppliers, contractors or external partners	At induction; every 2 years	MLRO / Finance Lead
Mandate fraud / invoice fraud awareness	Finance team and budget holders	At induction; annually	MLRO / Finance Lead
Modern slavery awareness (financial crime dimension)	Finance team; Manager of Student Services	Annually	MLRO / DSL
Governor AML briefing	All governors	On appointment; annually	MLRO / Principal

Training completion is recorded by the Registrar and reported to the Finance Board and the Board of Governors annually. Staff who have not completed mandatory AML and fraud awareness training may have access to financial systems restricted until training is completed.

25. Monitoring, Review and Governance

Activity	Lead	Frequency	Reported To
Annual policy review	MLRO / Finance Lead	Annual (April)	Board of Governors
AML risk assessment review	MLRO	Annual; after any significant incident	FAC; Board
SAR submissions log review	MLRO	Quarterly	FAC
Fraud incident log review	Finance Lead	Quarterly	Principal / CEO; FAC
Gifts and hospitality register review	Finance Lead	Quarterly	FAC
Training completion report	MLRO / Registrar	Annual	FAC; Board
Supplier due diligence register review	Finance Lead	Annual	MLRO
Financial controls audit (internal)	Internal auditor / Finance Lead	Annual	FAC
AML compliance report to Board	MLRO / Finance Lead	Annual	Board of Governors
Review of NCA / HMRC guidance updates	MLRO	Annual; as guidance is published	MLRO; Principal

26. Data Accuracy Assurance for Public Funding Submissions

EDA College's Data Accuracy Assurance Policy sits alongside this Policy and addresses, specifically, the accuracy of data the College submits to external organisations in connection with public funding. It has been developed to meet OfS initial condition E8.3.b, which requires comprehensive arrangements for detecting, preventing and stopping conduct that could amount to a relevant fraud offence or the inappropriate use of relevant public funds. This section summarises the salient elements of that Policy; the full Data Accuracy Assurance Policy should be read for complete detail.

26.1 Scope: Data Submitted to Third Parties Linked to Public Funding

This applies to all data submitted by or on behalf of the College where that data is used, directly or indirectly, to determine eligibility for, or the release, continuation or repayment of, relevant public funds, including data submitted to the following bodies:

Third Party	Data Submitted	Purpose / Public Funding Link	Frequency
Student Loans Company (SLC)	Student registration, attendance/engagement confirmation, course and enrolment data	Determines eligibility for, and release of, tuition fee loan payments to the College/BNU	Termly / as required
Birmingham Newman University (BNU)	Student attendance, assessment and progression data supporting sub-contractual funding claims	Underpins BNU's own reporting to SLC and OfS in respect of sub-contracted provision	Monthly and at census points
Office for Students (OfS)	Student number and financial data, quality and standards evidence	Registration, ongoing condition compliance and funding-related regulatory reporting	As required by OfS schedule
HESA / other statutory bodies	Student record returns (where applicable)	Statutory data return underpinning sector funding and regulatory oversight	Annual

26.2 Governance and Controls: From Data Capture to Submission

Overall accountability for the accuracy of data submitted to third parties in connection with public funding rests with the Accountable Officer. The College operates a staged control process for any such submission, and no submission may bypass the stages below:

Control Stage	Control Activity	Evidence Retained
1. Data capture	Source data entered directly by the individual responsible (tutor, administrator) at point of activity, using controlled system fields — no free-text override of key fields such as attendance status or enrolment dates	System audit log; user ID and timestamp on each entry
2. Independent validation	A second, independent staff member checks a sample (minimum 10%, or 100% for the first submission in an academic year) of records against source evidence before submission	Completed validation checklist, signed and dated
3. Reconciliation	Aggregate figures reconciled against underlying student records and finance system totals; any variance investigated and resolved before submission	Reconciliation worksheet retained for audit
4. Approval and sign-off	Data is not released externally until approved in writing by the Accountable Officer or their nominated deputy	Approval record (portal log or signed sign-off sheet)
5. Submission	Data submitted only via the approved secure channel for the relevant body (e.g. SLC portal, OfS portal); no ad hoc email submissions of funding-related data	Submission confirmation/receipt from receiving body
6. Post-submission review	Quarterly sample audit of submitted data against source records, carried out by a person independent of the original submission	Audit report to Risk and Compliance Board
7. Error correction	Any identified inaccuracy is corrected at source, the relevant third party notified without undue delay, and the error and correction logged	Error log with root cause and corrective action

26.3 Data Accuracy Principles

All staff involved in the data submission process must apply the following principles:

- Accuracy at source: data is recorded accurately and promptly at the point of the underlying activity, not retrospectively reconstructed
- No amendment without audit trail: any amendment to previously submitted or captured data is made through the College's system of record, with the reason and the identity of the person making it logged automatically
- Segregation of duties: the person who enters or amends source data must not be the same person who approves its external submission
- Independent verification: a sample of data is independently checked against source evidence before every submission
- Escalation of doubt: any member of staff uncertain about the accuracy of data, or who suspects it may have been manipulated, must escalate this immediately before submission proceeds
- Timely correction: any inaccuracy identified after submission is corrected at source and the relevant third party notified without undue delay

26.4 Escalation, Whistleblowing and Monitoring

Any member of staff, student or third party who suspects that inaccurate data has been, or is about to be, submitted to a third-party organisation in connection with public funding should raise this immediately through the College's Whistleblowing arrangements referred to in Section 22 of this Policy. Concerns may be raised without fear of detriment and, where preferred, anonymously. Staff with a role in capturing, validating, approving or submitting in-scope data must complete induction training on data accuracy before undertaking that role, and refresher training at least annually, in line with Section 24 of this Policy. The operation of these controls is subject to quarterly sample audit, an error log recording every identified inaccuracy and its correction, and an annual effectiveness review reported to the Risk and Compliance Board and the Governing Body, alongside the monitoring and governance arrangements set out in Section 25.

> Where a failure to follow data accuracy controls results, or could result, in the inappropriate use of public funds, the matter will additionally be treated as a suspected fraud under this Policy and may be reported to the relevant funding body and/or the Office for Students in accordance with the College's ongoing notification obligations.

Appendix A: Suspicious Activity Report (SAR) — Internal Form

Complete this form when you have knowledge or suspicion (or reasonable grounds for either) that a person is engaged in money laundering or terrorist financing. Submit to the MLRO immediately by hand or secure email. This form is STRICTLY CONFIDENTIAL. Do not discuss its contents with anyone other than the MLRO.

SECTION A: YOUR DETAILS	
Your name and role	
Date and time of this report	
Date and time of verbal report to MLRO (if made)	
Your contact details	
SECTION B: DETAILS OF THE PERSON / TRANSACTION OF CONCERN	
Name of the person you suspect (if known)	
Their relationship to EDA College (e.g. student, applicant, supplier, sponsor)	
Student ID or other reference (if applicable)	
Date(s) of the transaction or activity of concern	
Amount(s) involved (if applicable)	
Nature of the transaction (e.g. payment of fees, refund request, cash payment)	
SECTION C: NATURE OF YOUR SUSPICION	
Please describe in full what you know or suspect, and the specific facts or indicators that gave rise to your suspicion:	
What is the basis of your suspicion? (tick all that apply):	[ ] Unusual payment method or source [ ] Overpayment then refund request [ ] Identity document concerns [ ] High-risk jurisdiction [ ] Structuring / smurfing [ ] Evasive behaviour [ ] Third-party payment concerns [ ] Other (describe below)
Has any transaction already taken place?	Yes / No — If yes, describe:
Is a transaction about to take place?	Yes / No — If yes, describe and CONTACT THE MLRO IMMEDIATELY before proceeding
Has any evidence been preserved? If so, describe:	
Are there any other relevant persons or witnesses?	

SECTION D: DECLARATION	
I confirm that:	The information in this form is accurate to the best of my knowledge. I have not disclosed this concern to the person suspected or to any other person other than the MLRO. I understand that tipping off is a criminal offence. Signature / Name: ______________________________ Date: ___________
FOR MLRO USE ONLY	
Date received by MLRO	
MLRO assessment	
Action taken	[ ] No further action (reasons below) [ ] SAR submitted to NCA [ ] DAML requested [ ] Other
Reasons / NCA reference (if SAR submitted)	
Date of NCA submission (if applicable)	
MLRO signature	

Appendix B: Fraud Risk Register Template

The Fraud Risk Register is maintained by the Finance Lead and reviewed at each Finance Board meeting. It records identified fraud risks, existing controls, residual risk and any additional actions required.

Risk ID	Fraud Risk Description	Inherent Risk (H/M/L)	Existing Controls	Residual Risk (H/M/L)	Owner	Further Action Required	Review Date
FR-01	Ghost student / SLC fraud	HIGH	Attendance monitoring; enrolment verification; SLC reconciliation	MEDIUM	Finance Lead	Annual SLC reconciliation audit	Quarterly
FR-02	Mandate / invoice fraud	HIGH	Bank detail change verification procedure; dual authorisation	MEDIUM	Finance Lead	Staff training on mandate fraud	Annual
FR-03	Payroll fraud	MEDIUM	HR-payroll reconciliation; dual authorisation; external audit	LOW	Finance Lead	N/A	Annual
FR-04	Expense fraud	MEDIUM	Receipt requirement; line manager approval; Finance Lead of Finance review	LOW	Finance Lead	Random sample check quarterly	Quarterly
FR-05	Procurement fraud	MEDIUM	Procurement thresholds; tender process; conflict of interest declaration	LOW	Finance Lead	Supplier due diligence review	Annual
FR-06	Cyber / phishing fraud	HIGH	IT security; staff training; multi-factor authentication; incident response	MEDIUM	IT Lead	Phishing simulation exercise	Annual
FR-07	Money laundering (tuition fees)	MEDIUM	No cash fees; payment source verification; MLRO; SAR procedure	LOW	MLRO	AML risk assessment review	Annual
FR-08	Grant fraud	MEDIUM	Grant terms review; restricted fund accounting; external audit	LOW	Finance Lead	Grant compliance review	At grant closure

Appendix C: Red Flags Quick Reference for Staff

Print and keep accessible. For full guidance, see Sections 9 and 14 of this policy. If you see a red flag, report it to the MLRO or Finance Lead *immediately.*

Red Flag	What It May Indicate	Action
Payment of fees in cash or via unusual channels	Money laundering (placement)	STOP. Report to MLRO before accepting payment
Overpayment followed by refund request to different account	Money laundering (layering)	STOP. Report to MLRO. Do NOT process refund
Request to change supplier bank details by email	Mandate / invoice fraud	STOP. Verify by telephone to known number. Report to Finance Lead
Unexpected email requesting urgent payment	Business email compromise / phishing	STOP. Verify by telephone. Report to IT Lead
Unknown third party paying student's fees	Possible money laundering; student finance fraud	Report to MLRO before accepting payment
Student has no apparent genuine academic purpose	Possible ghost student / money laundering	Report to MLRO and Registry
Supplier invoice from unknown company	Possible invoice fraud	Verify supplier independently. Report to Finance Lead
Colleague asking you to bypass financial controls	Possible internal fraud	Refuse. Report to Finance Lead or Principal / CEO
Request for receipt or invoice that does not reflect reality	Possible tax evasion facilitation	Refuse. Report to MLRO
Signs a student's finances are controlled by another person	Possible modern slavery / money laundering	Report to DSL AND MLRO
Offer of gift, payment or favour from a supplier	Possible bribery	Decline. Record in Gifts Register. Report to Finance Lead
Clicking a suspicious link / email appearing to be phishing	Possible cyber attack	Report to IT Lead immediately. Do not click or respond

In all cases: DO NOT confront the person you suspect. DO NOT tell them you are making a report. DO NOT investigate yourself. REPORT to the MLRO immediately and preserve all evidence.

Appendix D: Key Contacts and Reporting Routes

Internal EDA College Contacts

Role	Contact	For
MLRO (Finance Lead and Operations)	Via College main office (marked 'PRIVATE AND CONFIDENTIAL — MLRO')	All AML suspicions; SAR submissions; AML policy queries; fraud reports
IT Lead	Via College main office	Cyber fraud; phishing; IT security incidents
Designated Safeguarding Lead	Student Engagement Lead	Modern slavery; student vulnerability connected to financial crime
Chair of Finance Board	Via Clerk to the Board	Concerns involving the Finance Lead or Principal / CEO
Chair of Board of Governors	Via Clerk to the Board	Serious governance or fraud concerns at senior leadership level

External Reporting Contacts

Organisation	Contact Details	For
National Crime Agency (NCA) — SAR submission	www.nationalcrimeagency.gov.uk/submit-a-sar | 0370 496 7622	Suspicious activity reports (SARs) for money laundering and terrorist financing
Action Fraud (national fraud reporting centre)	0300 123 2040 | www.actionfraud.police.uk	All fraud reports; mandate fraud; cyber fraud; identity fraud
HMRC Fraud Hotline	0800 788 887 | www.gov.uk/report-tax-fraud	Tax evasion; VAT fraud; PAYE fraud
Student Loans Company Fraud Team	studentfinancefrauda@slc.co.uk | www.slc.co.uk	Student finance fraud; ghost students; false SLC claims
Serious Fraud Office (SFO)	0207 239 7272 | www.sfo.gov.uk	Large-scale or complex fraud; bribery; corruption (typically above £1 million)
Crimestoppers	0800 555 111 (anonymous) | www.crimestoppers-uk.org	Anonymous reporting of any crime
Office for Students (OfS)	www.officeforstudents.org.uk | enquiries@officeforstudents.org.uk	Concerns about regulatory compliance affecting EDA College's OfS registration

Document ends here!