



Anti-Financial Crime Policy

Version 9.0



Contents

Version Control.....	2
Introduction.....	3
Purpose.....	3
Who and what this policy applies to.....	3
Definitions.....	4
Roles and Responsibilities.....	5
Directors (Nominated Officers).....	5
All Staff.....	5
Policy.....	6
Training and Awareness.....	6
Reporting and Whistleblowing.....	6
Tipping Off.....	6
Policy Controls.....	7
Bribery and Corruption.....	7
Offering and Accepting Gifts and Hospitality.....	7
Money Laundering.....	8
Terrorist and Proliferation Financing.....	8
Tax Evasion.....	9
Fraud.....	9
Managing Conflicts of Interest.....	10
Staff Training, Communication, and Awareness.....	10
Procedure for Reporting Financial Crime.....	11
Non-Compliance.....	12
Monitoring and Reviewing.....	12
Appendix A: Example Risks to Pathways LDN.....	13



Version Control

VERSION	REVIEWER NAME	DATE	NEXT REVIEW	COMMENTS
1.0	Rena Panesar	Sept 2016	Sept 2017	First Policy.
2.0	Rena Panesar	Sept 2017	Sept 2018	Updated.
3.0	Rena Panesar	Sept 2018	Sept 2019	Updated
4.0	Rena Panesar	Sept 2019	Sept 2020	Updated
5.0	Rena Panesar	Sept 2020	Sept 2021	Updated
6.0	Rena Panesar	Sept 2021	Sept 2022	Updated
7.0	Rena Panesar	Sept 2022	Sept 2023	Updated
8.0	Rena Panesar	Sept 2023	Sept 2024	Updated
9.0	Policy Pros	Oct 2025	Oct 2026	Retamplated and expanded from Anti-Fraud to include other financial crimes.



Anti-Financial Crime Policy

Introduction

Pathways LDN is committed to the highest standards of financial integrity, accountability, and ethical conduct. As an Independent Training Provider (ITP) in receipt of public funds from the Department for Education (DfE) and the Education and Skills Funding Agency (ESFA), we have a legal and ethical duty to ensure public money is used solely for its intended purpose—the delivery of high-quality education and training.

We operate a **zero-tolerance policy** towards fraud, bribery, corruption, money laundering and all forms of financial crime. This policy applies rigorous controls to prevent, detect, and respond to all forms of financial misconduct.

Purpose

The purpose of this policy is to:

- Ensure the proper and effective stewardship of DfE/ESFA (public) funds and other assets for which Pathways LDN is responsible.
- Establish procedures to comply with UK legislation, including the Bribery Act 2010, Fraud Act 2006, and the requirements set out in the DfE/ESFA Financial Handbook for ITPs.
- Maintain the trust and confidence of our learners, employers, and funding partners by ensuring transparent and ethical financial management.
- Equip all staff with the knowledge to identify, manage, and report instances of suspected financial misconduct and error.

Who and what this policy applies to

This policy applies to all individuals working for or on behalf of Pathways LDN.

The policy covers all financial and non-financial transactions and activities, including those related to procurement, employment, expense claims, learner enrolment, and funding data submissions (ILR).



Definitions

Bribery: The offering, giving, receiving, or soliciting of anything of value (such as gifts, money, favours, or hospitality) with the intention of influencing the actions of an individual in a position of trust. Bribery is a criminal offence under the **Bribery Act 2010** and includes facilitation payments and kickbacks.

Corruption: The abuse of entrusted power for private gain. Corruption may involve bribery, but also includes acts such as fraud.

Money Laundering: The process of disguising the origin of criminal property to make it appear legitimate. It includes acquiring, using, possessing, or transferring criminal funds, and failing to report suspicious activity under the **Proceeds of Crime Act 2002 (POCA)**.

Terrorist Financing: The act of providing or collecting funds, by any means, directly or indirectly, with the intention or knowledge that they will be used to support terrorist acts or organisations. This is a criminal offence under the **Terrorism Act 2000**.

Proliferation Financing: The act of providing funds or financial services that are used, in whole or in part, for the development, production, or acquisition of nuclear, chemical, or biological weapons, in breach of international obligations.

Tax Evasion: The illegal practice of not paying taxes by deliberately misrepresenting or concealing information to reduce tax liability. This includes actions such as underreporting income, inflating deductions, or hiding money in offshore accounts. Under the **Criminal Finances Act 2017**, it is also a corporate offence to fail to prevent someone associated with the company from facilitating tax evasion.

Our policy is simple – **zero tolerance** to any form of financial crime!



Roles and Responsibilities

Directors (Nominated Officers)

- Approve the Anti-Financial Crime Policy and related controls and procedures.
- Ensure compliance with the Bribery Act, POCA, CFA 2017, Fraud Act, and ESFA rules.
- Ensure due diligence on medium to high-risk partners and suppliers.
- Maintain registers of interests and gifts.
- Mandate appropriate training on the subject for all staff.
- Escalate concerns and/or wrongdoing to ESFA, the police, the NCA, etc.
- Chair quarterly compliance reviews and facilitate improvements as required.

All Staff

- Complete the required training and follow policy and procedures.
- Always act with honesty and integrity.
- Declare conflicts, gifts and hospitality.
- Maintain vigilance.
- Report suspicions at once to a Director.



Policy

Training and Awareness

While Pathways LDN Ltd. operates in a low-risk sector, it will ensure that the Directors and its staff are made aware of the risks of financial crime and how to report concerns.

This may include reading this policy and related procedures, reading related sector guidance, attending periodic briefings, updates, etc.

Reporting and Whistleblowing

Any concerns about actual or suspected financial crime must be reported immediately to the Directors. Reports can be made confidentially and without fear of retaliation (via our Whistleblowing Policy).

Where appropriate, concerns will be reported directly to law enforcement or regulatory bodies by the Directors.

Tipping Off

It is a criminal offence for anyone to say or do anything that may prejudice an investigation or 'tip off' another person that a suspicion has been raised, a suspicious activity report has been submitted or that a money laundering or terrorist financing investigation may be carried out. It is also an offence to falsify, conceal or destroy documents relevant to investigations.

Nobody should tell or inform the person involved in the transaction or anyone else that:

- The transaction is being or was delayed because a suspicion has been raised.
- Details of a transaction have or will be reported to the National Crime Agency.
- Law enforcement agencies are investigating the individual/organisation.

Such an offence carries a penalty of up to 5 years imprisonment, a fine or both.



Policy Controls

Bribery and Corruption

Pathways LDN prohibits the offering, giving, soliciting, or receiving of any bribe or improper advantage, whether directly or indirectly. This includes:

- Offering or accepting gifts, hospitality, or other benefits intended to influence decision-making;
- Facilitating payments made to expedite routine government actions;
- Engaging in corrupt practices when tendering, contracting, or managing suppliers or subcontractors.

Offering and Accepting Gifts and Hospitality

It is our policy that gifts and hospitality should not routinely be offered and accepted. However, we recognise that there may be occasions where token gifts may be handed out at conferences or thank you cards may be given to staff by learners as a thank you. Likewise, we recognise that we may offer or be offered refreshments at meetings when hosting or being hosted by our partners. Therefore, these may be offered and accepted so long as they meet the following requirements:

- They are not made to directly influence the party to whom it is being given.
- They are not made with the suggestion that a return favour is expected.
- They follow local law.
- They follow the policy of the receiving party.
- They do not include cash or a cash equivalent.
- They are of an appropriate type and value (under £10 per head in value).
- They are given at an appropriate time (e.g., at Christmas, to say 'thank you' or at a meeting where negotiations are not taking place).
- They are given/received openly, not secretly.
- They are recorded in the Gifts and Hospitality Register by the Directors.



Anti-Financial Crime Policy

Money Laundering

Although Pathways LDN operates in a low-risk sector and is not subject to the Money Laundering Regulations 2017, the company recognises its responsibilities under the Proceeds of Crime Act 2002 (POCA). Money laundering can occur in any business environment, and Pathways LDN is committed to preventing its operations from being used to disguise the origins of criminal property.

To that end, Pathways LDN will:

- Refuse to accept payments in cash or from unknown third parties.
- Ensure that all financial transactions are conducted through recognised UK financial institutions.
- Remain alert to suspicious behaviour or payment patterns.
- Maintain accurate records of all payments into and out of the business.
- Report any suspicions of money laundering to the National Crime Agency (NCA) through appropriate channels.

While the risk is low, the Directors are aware of and prepared to submit a Suspicious Activity Report (SAR) should the need arise.

Terrorist and Proliferation Financing

Pathways LDN will not knowingly facilitate the funding of terrorism or the proliferation of weapons of mass destruction. We will:

- Remain alert to any unusual or high-risk patterns of activity, including those involving high-risk jurisdictions or politically exposed persons (PEPs).
- Report any suspicions in line with the Terrorism Act 2000 and relevant sanctions legislation.

We will also, where appropriate, and a business relationship is high risk (the partner operates in a high-risk region, a PEP is a person with significant control, etc.):

- Carry out customer (supplier or partner) due diligence.
- Screen our transactions and relationships against UK and international sanctions lists.



Anti-Financial Crime Policy

Tax Evasion

Pathways LDN fully complies with UK tax laws and the obligations imposed by the Criminal Finances Act 2017, which makes it a criminal offence for companies to fail to prevent the facilitation of tax evasion.

Pathways LDN prohibits:

- Any direct or indirect facilitation of tax evasion.
- Engaging with individuals or businesses that refuse to confirm their own tax compliance.
- Accepting or making off-record payments or false invoicing.

All financial activities are fully transparent and documented. Invoices, payroll records, and subcontractor agreements are maintained to provide a clear audit trail. Any suspicions of tax evasion will be reported to HMRC without delay.

Fraud

Pathways LDN maintains a strong, robust system to prevent fraud, strictly adhering to a zero-tolerance policy.

- Compliance with DfE/ESFA funding rules is safeguarded through preventative controls like dual authorisation for all payments and a robust procurement process.
- Detection is handled proactively through regular internal spot checks by the Quality & Compliance team, led by Rena Panesar, with the ability to involve the company accountant for deeper investigations.
- All funding claims, including those from external contracts, are subjected to internal quality checks before external funder audits.
- Crucially, the policy mandates that the Directors must immediately notify the DfE/ESFA of any suspicion or irregularity involving public funds, ensuring swift action is taken to uphold financial integrity and accountability.



Managing Conflicts of Interest

While a conflict of interest is not automatically a financial crime, it is a common route into it and a clear red flag. When a person's private interests (personal or financial) compete with their duty to act for Pathways LDN and safeguarding the use of public funds, controls can be bypassed, decisions can be biased, and public funds can be misused.

For example:

- An employer offers gifts or hospitality to secure learner referrals for apprenticeships – this would be a conflict if that employer may not be best suited to take learners on.
- A staff member involved in procurement decides to purchase IT equipment from a business owned by a family member – this would be a conflict if the IT equipment purchased is not demonstrably the best value, does not meet the specification, etc.

Therefore, all staff must declare any actual or potential conflicts of interest to the Directors. This is particularly important if the staff member is involved in partnership and procurement decisions.

Following any declaration, the Directors will determine how best to manage the conflict.

Staff Training, Communication, and Awareness

Pathways LDN is committed to ensuring that all personnel possess the necessary knowledge and awareness to actively prevent, detect, and respond to financial crime. Our training strategy is designed to be comprehensive, practical, and regularly reinforced.

We utilise a blended approach to maximise engagement and accessibility, offering training both online and in-person.

Training is tailored to specific roles, with enhanced and specialised training provided to key personnel, including Directors, Finance staff, Procurement teams, and the Quality & Compliance team.



Procedure for Reporting Financial Crime

Step 1: Report internally first, and fast

- Even if you just have a suspicion, tell a Director immediately. Use the whistleblowing route if you prefer.
- Do not investigate yourself, and do not alert the subject.

Step 2: Internal investigation

Where appropriate, we will investigate the matter or engage an independent third-party to investigate on our behalf.

Step 3: We report the matter externally

- **Fraud or cybercrime** will be reported to **Action Fraud**.
- **Money laundering or suspicious funds** will be reported via a **Suspicious Activity Report** to the **NCA**.
- **Suspected facilitation of tax evasion** will be reported to **HMRC**.
- **Bribery, corruption and other serious crimes** will be reported to the **police**.
- **ESFA-funded provision** – where public funds may be at risk, we will notify the **DfE/ESFA**.

No individual will suffer any detriment or retaliation for reporting a genuine concern in good faith, even if it turns out to be unfounded.



Non-Compliance

Pathways LDN takes any breach of this policy seriously, as non-compliance may result in reputational damage as well as the withdrawal of government funding.

Therefore, all individuals working for or on behalf of the business are expected to uphold the standards set out in this policy.

Failure to comply with the Anti-Financial Crime Policy may result in:

- Immediate termination of working, business or partnership relationships;
- Disciplinary action (for staff), up to and including dismissal;
- Referral to relevant authorities such as HMRC, the National Crime Agency, Police Scotland, or regulatory bodies;

Any instance of non-compliance will be investigated by the Director, with appropriate action taken depending on the nature and severity of the issue.

Where a breach is found to involve criminal conduct – such as bribery, tax evasion, or money laundering – Pathways LDN will cooperate fully with law enforcement and regulatory agencies and may seek legal advice to support enforcement and remediation.

Monitoring and Reviewing

Pathways LDN Ltd. is committed to ensuring our policies are effective and up-to-date.

The Directors are responsible for this process and will review this policy at least once a year or more frequently if needed due to changes in laws, regulatory guidance, or best practice.



Appendix A: Example Risks to Pathways LDN

- Enrolment and eligibility fraud
 - Creating ghost learners; enrolling ineligible learners; backdating start dates to meet funding rules; duplicate funding across providers.
- Attendance and learning evidence fraud
 - False registers or online logins; fabricated off-the-job hours for apprentices; copied portfolios; coaching learners to sign paperwork they did not complete.
- Employer incentive and inducement risks
 - Paying or receiving improper inducements to secure starts; offering cash or gifts to employers or learners to influence recruitment or retention decisions.
- Subcontracting and partner abuse
 - Hidden or unmanaged subcontracting; passing funds to unapproved partners; inflated invoices for little or no delivery; circular payments between related parties.
- Conflicts of interest and related-party transactions
 - Directors or staff awarding contracts to their own companies or relatives without fair competition; undisclosed second jobs with partner organisations.
- Procurement and invoice fraud
 - Kickbacks for awarding contracts; false invoices; overbilling; split purchases to avoid approval limits; invoice redirection scams.
- Payroll and expenses fraud
 - Ghost employees; falsified overtime or mileage; personal expenditure on corporate cards; manipulated timesheets for delivery staff.
- Bursary and learner support misuse
 - Misuse of bursary funds, hardship payments, or device loans; cash withdrawals without receipts; reusing receipts.



Anti-Financial Crime Policy

- Bank mandate and payment diversion
 - Social engineering to change supplier bank details; fake refund requests; creation of bogus suppliers.
- Money laundering exposure
 - Acceptance of large cash payments for commercial courses; third-party payments that do not match the learner or employer; rapid refunds to different accounts.
- Bribery and corruption
 - Gifts, hospitality, or favours intended to influence audit outcomes, referrals, or contract awards; small but repeated "thank you" payments to staff.
- Criminal Finances Act 2017 risk
 - Failure to prevent the facilitation of tax evasion by learners, employers, suppliers, or staff, for example, false invoices to shift taxable income.
- Data manipulation before audit
 - Altering ILR data or evidence packs to pass funding audits; retrofitting signatures or timestamps.
- Asset misuse and theft
 - Loss or resale of laptops, tablets, or tools bought with public funds; private use of provider vehicles or fuel cards.
- Sanctions and restricted party risk
 - Engaging overseas partners or suppliers without screening for sanctions or politically exposed persons; payments that breach trade controls.
- Whistleblowing suppression
 - Discouraging or penalising staff who raise fraud concerns which increases undetected loss and regulatory penalties.