Quack
Recruitment & Training

Counter Fraud, Bribery, Corruption and Financial Irregularity Policy

Publicly Funded Training, Recruitment and Corporate Operations | Version 2.1

Policy field	Current position
Provider	Quack Recruitment & Training Ltd
Applies to	Directors, employees, workers, tutors, assessors, IQAs, learner engagement and progression staff, contractors, associates, learners, employers, suppliers, subcontractors, delivery partners and any person acting for or on behalf of Quack.
Policy owner	Jessica Roughton - Quality & Compliance Lead, DSL and SEND Lead
Senior accountable lead	Dion Bishop - Director of Contracts & Operations
Alternative escalation route	Independent Governor or a suitably independent external legal, accountancy, HR, safeguarding, awarding-organisation or compliance adviser where the usual decision-maker is implicated or lacks independence.
Approved systems and records	PICS, Microsoft 365, Highfield systems, Power BI, approved banking and accounting systems, learner and contract evidence folders, fraud and irregularity register, gifts and hospitality register, conflict-of-interest register, investigation files and QIP.
Related policies	Whistleblowing; Malpractice and Maladministration; Conflict of Interest and Related-Party Relationships; Information Security; GDPR and Learner Privacy; Disciplinary; Complaints; Assessment Appeals; IQA; Safer Recruitment; Examinations; Safeguarding and Prevent.
Effective date	6 August 2026
Next review	August 2027, or sooner following a suspected or confirmed incident, material contract or system change, legislation, funder or awarding-organisation update.

Policy intent

Quack will prevent, detect, report and respond to fraud, bribery, corruption and financial irregularity in a proportionate way that protects learners, public funds, assessment integrity, commissioners, employers and the business. Controls must be practical for a small family-run provider, but no relationship, target or commercial pressure justifies inaccurate evidence, improper influence, concealment or misuse of funds.

Quack Recruitment & Training

Contents

Use with operational records

This policy sets the control framework. It must be evidenced through normal operating records, including learner files, PICS and ILR reports, payment approvals, employer evidence, IQA records, bank-verification checks, declarations, audit trails, investigation records and corrective-action logs. A policy without implementation evidence does not provide assurance.

1. Purpose and Policy Intent

Quack Recruitment & Training Ltd is entrusted with public funding, learner and employer information, qualification evidence, supplier payments and company assets. This policy explains how Quack prevents, identifies, reports, investigates and responds to suspected fraud, bribery, corruption, theft, false accounting and other financial or evidential irregularity.

The policy applies equally where conduct is intended to benefit an individual, a connected person, Quack, a learner, an employer, a supplier or another organisation. An act does not cease to be fraudulent because the intended beneficiary is the company rather than the individual who carried it out.

The intended outcomes are that public and company funds are used only for legitimate purposes; learner, assessment and progression evidence is authentic; staff understand their reporting obligations; potential wrongdoing is contained quickly; affected records and claims are corrected transparently; and leaders use incidents and near misses to strengthen controls.

2. Scope and Application

Area	Examples within scope
Funded learner journey	Marketing, IAG, eligibility, residency, prior learning, enrolment, attendance, GLH, learner support, assessment, achievement, completion, progression and destination evidence.
Funding and performance data	PICS, ILR, occupancy reports, FIS/PDSAT checks, Power BI, FESIT, MS1/MS2/MS3 claims, invoices, reconciliation and commissioner reporting.
Assessment and certification	Learner work, invigilation, reasonable adjustments, IQA, EQA, registrations, certificate claims, authenticity and awarding-organisation communications.
Employer and progression activity	Vacancies, interviews, employer confirmations, contracts, payslips, job descriptions, employment starts, added responsibilities and outcome evidence.
Financial operations	Supplier onboarding, purchase approval, invoices, bank details, payroll, expenses, refunds, credit cards, assets, cash, tax, loans and insurance claims.
Recruitment and staffing	Applications, references, qualifications, timesheets, pay, bonuses, overtime, conflicts, recruitment fees and use of contractors.
Technology and data	Account access, phishing, payment diversion, cyber-enabled fraud, unauthorised alteration or deletion of records and use of AI to fabricate or manipulate evidence.
External relationships	Funders, auditors, Ofsted, awarding organisations, subcontractors, referral partners, employers, suppliers and professional advisers.

Honest error, poor practice, negligence, maladministration and deliberate fraud are not identical. All material discrepancies must be reported and corrected. The classification and response will depend on evidence, intent, recklessness, repetition, concealment, impact and legal or contractual duties.

3. Legal, Regulatory, Funding and Good-Practice Context

Framework	Relevance to Quack
Fraud Act 2006	Creates offences of fraud by false representation, failure to disclose information where there is a legal duty, and abuse of position. These may apply to false learner, funding, employer, supplier or financial representations.
Bribery Act 2010	Prohibits offering, promising or giving a bribe; requesting, agreeing to receive or accepting a bribe; bribing a foreign public official; and failure by a commercial organisation to prevent bribery by associated persons. Prevention procedures should be proportionate, risk-based and actively monitored.
Economic Crime and Corporate Transparency Act 2023	Introduced the corporate failure-to-prevent-fraud offence for large organisations from 1 September 2025. Quack may not meet the statutory size threshold, but adopts the reasonable-procedures principles as good practice and may be required to provide assurance when acting for larger clients or public bodies.
Theft Act 1968 and Companies Act 2006	Relevant to theft, false accounting, false statements, fraudulent trading, directors' duties and responsible stewardship of company assets and records.
Criminal Finances Act 2017	Requires relevant bodies of all sizes to consider reasonable procedures to prevent associated persons criminally facilitating tax evasion.
UK GDPR and Data Protection Act 2018	Fraud prevention, investigation and evidence handling must use personal data lawfully, securely, proportionately and with appropriate access restrictions.
Skills Bootcamp contracts and public-funding requirements	Claims, learner records, evidence and commissioner communications must be accurate, timely, complete and capable of independent verification. Suspected or confirmed irregularity may require prompt disclosure and correction.
Awarding-organisation and Ofqual requirements	Assessment, registration, certification and quality-assurance records must be authentic and protected from malpractice, conflicts and improper influence.
GovS 013 Counter Fraud	Applies directly to government bodies rather than Quack, but provides relevant good-practice principles on fraud risk assessment, prevention, detection, response, learning and assurance.

Framework	Relevance to Quack
Proportionate application This policy does not claim that every statutory corporate offence applies to Quack in every circumstance. Where legal scope is uncertain, leaders will obtain appropriate professional advice. The operational standard remains that Quack will not tolerate dishonest conduct and will maintain controls proportionate to its risks and size.	

4. Definitions

Term	Meaning for this policy
Error	An unintended inaccuracy or omission without evidence of dishonesty. Errors must still be corrected and may identify control weaknesses.
Irregularity	Activity or a record that departs from law, contract, policy, procedure or expected control. It may be accidental, negligent, reckless or deliberate.
Fraud	Dishonest conduct intended to make a gain, cause a loss or expose another to risk of loss, including false representation, dishonest non-disclosure or abuse of position.
Bribery	Offering, promising, giving, requesting, agreeing to receive or accepting a financial or other advantage to induce or reward improper performance.
Corruption	Abuse of entrusted power, influence, position or access for private, connected-person or organisational advantage.
Financial irregularity	An unexplained, unauthorised or improper transaction, claim, payment, accounting entry, asset use or failure to follow financial controls.
Collusion	Two or more people cooperating improperly to manipulate a process, conceal facts, submit false evidence or obtain an unfair advantage.
Associated person	A person or organisation performing services for or on behalf of Quack, which may include employees, agents, contractors, subsidiaries, consultants or intermediaries depending on the circumstances.
Public funds	Funding or payments originating from government, mayoral combined authorities, local authorities or other public bodies, including milestone and outcome payments.
Red flag	An indicator requiring review. A red flag is not proof of wrongdoing and must be assessed objectively.
Balance of probabilities	The internal civil standard used to decide whether it is more likely than not that conduct occurred. Criminal liability is determined only by the appropriate authorities and courts.

5. Policy Principles and Organisational Position

- Quack has zero tolerance for fraud, bribery and corruption. “Zero tolerance” means concerns are reported, assessed and addressed; it does not mean every error is automatically treated as deliberate misconduct.
- Leaders will set a clear tone that funding targets, cash-flow pressure, deadlines, commercial relationships or family relationships do not justify inaccurate claims, concealment or bypassing controls.
- Controls must be proportionate to Quack’s size. Where complete segregation of duties is impracticable, compensating controls such as second review, retrospective sampling, independent challenge and recorded rationale must be used.
- No person should, where reasonably practicable, create the evidence, approve it, submit the claim and authorise the resulting payment without another competent review.
- Original records and audit trails must be preserved. Corrections must be transparent and must not overwrite or destroy evidence of the original entry unless the system retains a complete audit history.
- Suspected wrongdoing will be handled fairly and confidentially. A concern is not a finding, and individuals must not be treated as guilty before evidence is reviewed.
- Good-faith reporters will be protected from retaliation. Deliberately false or malicious allegations may be addressed under relevant conduct procedures.
- Quack will cooperate with funders, awarding organisations, auditors, regulators, law enforcement and insurers where notification or assistance is required.
- Where an irregularity affects one learner, claim, assessor, employer or supplier, leaders will consider whether the same cause could affect a wider population.

6. Principal Fraud and Irregularity Risks

Risk area	Examples of prohibited or concerning activity	Core evidence / control
Eligibility and enrolment	Fabricated or altered identity, address, residency, employment status, prior learning, public-funds eligibility, signatures or declarations; duplicate enrolment; enrolling a person known to be ineligible.	Eligibility checklist, original evidence, PICS record, second-line file review, exception log.
Attendance and GLH	Signing for absent learners; recording full sessions that did not take place; retrospective fabrication; duplicate attendance; claiming learning that was not delivered.	Contemporaneous registers, Teams attendance, tutor records, learner voice, timetable and PICS reconciliation.
Assessment and achievement	Copied, AI-generated or fabricated work; assessor collusion; false feedback; claiming units not completed; improper examination assistance; unsupported certificates.	Learner work, authenticity checks, assessor records, IQA sampling, invigilation evidence and Highfield audit trail.
MS1/MS2/MS3 and progression	Fabricated interview, job, pay, contract or employer evidence; claiming an outcome outside contractual rules; altering dates; employer confirmation by an undisclosed connected person.	Learner and employer evidence, direct verification, SignNow/email audit trail, claim checklist and conflict declaration.
ILR and management information	Deliberate miscoding, omission or alteration to obtain payment, conceal underperformance or mislead a funder, auditor, governor or Ofsted.	PICS/ILR reconciliation, FIS/PDSAT, occupancy reports, Power BI/FESIT checks, correction log.
Invoices and suppliers	Fictitious supplier, duplicate or inflated invoice, split purchase, false service delivery, related-party concealment, kickback or unauthorised bank-detail change.	Approved supplier record, purchase evidence, bank verification, two-stage payment approval, conflict register.
Payroll, expenses and assets	Fictitious worker, false timesheet, inflated mileage, personal expenditure, duplicate claim, unauthorised bonus, theft or misuse of equipment.	Contracts, payroll records, receipts, manager approval, asset register and periodic review.
Cyber and payment diversion	Phishing, compromised email, fraudulent invoice, CEO impersonation, changed bank details, credential misuse or unauthorised system access.	Call-back verification, MFA, access logs, payment controls, Cyber Essentials controls and incident response.
Bribery and influence	Cash, gift, hospitality, favour, job opportunity, commission or other advantage offered or accepted to affect recruitment, award, assessment, claim, procurement or audit.	Gifts and hospitality register, conflict declaration, approval record, whistleblowing route.
External assurance	Destroying, withholding or fabricating evidence; coaching a person to mislead; knowingly making false statements to funders, auditors, awarding organisations, insurers or inspectors.	Document-control records, evidence-preservation hold, meeting notes, correspondence and investigation trail.

7. Prevention and Control Framework

7.1 Fraud risk assessment

The Quality & Compliance Lead and senior accountable lead will maintain a proportionate fraud-risk assessment covering funded delivery, claims, assessment, finance, procurement, payroll, cyber risk and connected-party activity. It will be reviewed at least annually and after a significant incident, new contract, system change, delivery-model change or material change in risk.

7.2 Segregation and compensating controls

Process	Expected separation	Where full separation is not practicable
Learner eligibility	One person gathers/checks evidence; a competent second-line sample or approval is completed before claim or within the agreed control cycle.	Document the exception; complete enhanced retrospective sample before submission or payment confirmation.
Milestone/outcome claim	Evidence owner compiles; authorised reviewer validates contractual compliance; claim submission is traceable.	Independent sample by Quality Lead, Director or external reviewer, with findings recorded before invoice approval where possible.
Supplier payment	Request/purchase, invoice approval, bank-detail verification and payment authorisation are separated where possible.	Second authoriser or documented post-payment review; no bank-detail change accepted solely by email.
Assessment/certification	Assessor decision, IQA, registration/certification and conflict management follow awarding-organisation rules.	Increase sampling, use another competent IQA or seek awarding-organisation/external support.
Payroll/expenses	Claimant does not approve own claim. Material or unusual payments receive second review.	Owner/director approval supported by receipts, contract and independent accountancy review where appropriate.

7.3 Required preventative controls

- Use only approved systems and current controlled forms; restrict access according to role and remove access promptly when duties change or employment ends.
- Keep evidence contemporaneously wherever possible. Late or reconstructed records must be clearly identified, explained and independently checked; they must never be presented as contemporaneous if they are not.
- Verify supplier and employee bank-detail changes using a trusted telephone number or another independent route, not the contact details contained only in the change request.
- Complete data-quality and funding checks before submission and retain evidence of errors, corrections, owners and closure.

- Complete due diligence proportionate to risk for suppliers, subcontractors, employer partners, agents and consultants, including ownership, bank details, capability, conflicts and safeguarding where relevant.
- Use written contracts, purchase orders, job descriptions, pay approvals and deliverables for material arrangements.
- Maintain a Conflict of Interest and Related-Party Register and apply the related policy to procurement, employment, assessment and funding decisions.
- Require staff to complete induction and periodic refresher training on fraud, bribery, cyber risk, whistleblowing, data quality and funding evidence relevant to their role.
- Use learner, employer, staff and supplier feedback, data analysis and internal audit to identify anomalies and emerging risks.
- Do not pay cash, facilitation payments, secret commissions or unrecorded incentives.

8. Bribery, Gifts, Hospitality and Improper Influence

No person acting for Quack may offer, promise, give, request, agree to receive or accept an advantage intended to induce or reward improper performance. This applies to dealings with public officials, funders, employers, learners, awarding organisations, suppliers, auditors and private organisations in the UK or overseas.

Position	Requirement
Cash and cash equivalents	Cash gifts, vouchers readily exchangeable for cash, personal transfers, loans, secret commissions and facilitation payments are prohibited.
Gifts and hospitality under £25	May be accepted only where modest, infrequent, lawful, transparent and incapable of influencing a decision. Repeated or sensitive gifts must still be declared.
Gifts or hospitality of £25 or more	Must be declared promptly and approved before acceptance where practicable. The register records value, source, purpose, decision and any mitigation.
During procurement, audit, assessment, recruitment or funding decision	Gifts or hospitality from an interested party should normally be refused regardless of value, except ordinary low-value refreshments provided openly at a meeting.
Travel, accommodation or event attendance	Requires prior written approval where paid by an external party. The business purpose, cost, relationship and conflict risk must be considered.
Donations, sponsorship or discounts	Must not be used to secure improper influence. Material arrangements require written terms, due diligence and conflict review.
Offers made to Quack staff	The offer must be recorded even if refused where it could reasonably be viewed as an attempt to influence a decision.

No target pressure defence

A payment target, contract deadline, performance concern or fear of losing funding is never a justification for altering, fabricating, withholding or misrepresenting evidence.

9. Reporting Suspected Fraud or Irregularity

Anyone may raise a concern. Staff must report suspected fraud, bribery, corruption, theft or material financial irregularity promptly and must not wait until they can prove it. Learners, employers, suppliers and external stakeholders may also use the complaint or whistleblowing routes.

Route	When to use
Line manager or Quality & Compliance Lead	Normal route for an error, anomaly, suspicious evidence, data discrepancy, assessment concern or financial irregularity.
Senior accountable lead - Dion Bishop	Serious, systemic, financially material or externally reportable concern, or where immediate authority is required to protect funds or evidence.
Independent Governor / external adviser	Where the concern implicates Dion, Jessica, another usual decision-maker, a connected person, or where a competent independent internal investigator is unavailable.
DSL / Deputy DSL	Where conduct also creates a safeguarding, Prevent, exploitation, modern-slavery or learner-welfare risk.
Whistleblowing route	Where the reporter reasonably believes wrongdoing is in the public interest, fears retaliation, believes normal management may conceal the issue or has raised it without adequate response.
Emergency / external route	Call 999 for immediate danger or active crime. Contact the bank, insurer, cyber-response service, police/Report Fraud or relevant authority promptly where delay could increase loss or harm.

- Do not confront a suspected person, conduct covert surveillance, access accounts without authority or attempt to recover deleted material without specialist support.
- Do not delete, amend, backdate, replace or “tidy” the relevant records. Preserve emails, messages, files, system logs, paper records and device information lawfully.

- Record facts, dates, people, systems, values, learner or contract references and the immediate risk. Separate observation from assumption.
- Where an incorrect claim or record is identified, report it immediately. Correction can begin to protect public funds, but the original audit trail and investigation evidence must be retained.

10. Triage, Investigation and Decision-Making

10.1 Initial triage

The receiving manager must acknowledge the concern as soon as reasonably practicable and normally within two working days. Immediate triage will determine whether to protect a learner, suspend a payment or claim, preserve evidence, restrict system access, notify the bank or insurer, seek legal advice, involve the DSL, or make an external notification.

Triage question	Action consideration
Is there immediate risk of harm, loss or evidence destruction?	Take proportionate interim action without waiting for a full investigation. Record who authorised it and why.
Does the concern involve public funding or qualification integrity?	Consider commissioner, DfE, awarding-organisation, EQA or regulator notification and hold affected claims/certification.
Is the usual investigator conflicted or implicated?	Appoint an independent competent investigator or obtain external support.
Could the issue be wider than one record?	Define a risk-based population sample and consider full review where evidence indicates systemic exposure.
Is criminal conduct reasonably suspected?	Seek legal/professional advice and consider police, Report Fraud, SFO or other appropriate reporting route. Do not compromise a criminal investigation.
Is personal data involved?	Apply the data-breach process and assess ICO/individual notification within statutory timescales.
Does the matter involve an employee?	Coordinate with disciplinary, grievance, whistleblowing and safeguarding procedures; interim action is neutral and not a finding.

10.2 Investigation standards

- The investigator must be competent, impartial and free from material personal interest. Terms of reference will define allegations, scope, authority, records, reporting line and timescale.
- The investigation will be proportionate to the risk and may include document review, system logs, data analysis, learner/employer verification, interviews, financial reconciliation and external specialist evidence.
- Individuals whose conduct is under review will normally be given a fair opportunity to respond, subject to lawful restrictions needed to protect evidence, safeguarding or a criminal/regulatory investigation.
- Internal findings will be made on the balance of probabilities and will distinguish substantiated, partially substantiated, unsubstantiated and inconclusive matters.
- A straightforward internal review should normally be completed within 20 working days. Complex cases may take longer; reasons, risk controls and progress updates must be recorded.
- The investigator will not amend source evidence. Working copies, redactions and analysis must be clearly controlled.
- The final report will set out scope, methodology, evidence, findings, financial or learner impact, wider-population risk, notifications, recovery, control failures and required actions.

10.3 Interim measures

Interim measures may include suspending a claim, payment, certification or system access; securing records; changing duties; pausing an employer or supplier relationship; or suspending an employee on full pay where appropriate. Measures must be necessary, proportionate, reviewed regularly and must not be presented as a finding of guilt.

11. External Notification, Correction and Recovery

Recipient / action	Trigger and expectation
Commissioner or funder	Notify where contract, funding rules, audit terms or materiality require it; provide accurate facts, affected population, immediate controls, correction plan and updates.
Awarding organisation / EQA / Ofqual	Notify suspected assessment, examination, registration, certification or centre malpractice in accordance with applicable rules and directions.
Police / Report Fraud / Serious Fraud Office	Consider where criminal fraud, bribery, corruption or serious economic crime is suspected. Obtain legal advice for complex or high-value matters.
Bank, payment provider and insurer	Contact immediately where payment diversion, account compromise, card fraud, cyber incident or recoverable loss may have occurred.
ICO and affected individuals	Assess and notify in accordance with the personal-data-breach procedure where rights and freedoms are at risk.
HMRC or professional advisers	Use where tax, payroll, false accounting, company-law or professional-reporting obligations may arise.

Recipient / action	Trigger and expectation
Correction of records and claims	Correct PICS, ILR, invoice, funding, assessment, certificate or financial records transparently; retain the original audit trail; identify owner, date, reason and external confirmation.
Recovery and sanctions	Seek repayment, set-off, insurance recovery, civil action, disciplinary sanction, contract termination, qualification action or referral to professional/regulatory bodies where lawful and proportionate.

Self-reporting and correction should not be delayed merely because the investigation is incomplete where delay would knowingly maintain an inaccurate claim, payment or certificate. The notification must distinguish confirmed facts from matters still under investigation.

12. Protection of Learners, Staff and Evidence

- Learners unaffected by wrongdoing must not be penalised. Quack will protect access to learning, assessment, evidence and certification wherever possible.
- Where learner work or employer evidence is in doubt, decisions will be individualised and supported by re-assessment, re-verification or alternative evidence where permitted, rather than assuming all learners are involved.
- Reporters and witnesses will be treated respectfully and protected from retaliation. Confidentiality will be maintained so far as possible, but cannot be guaranteed where disclosure is required by law or fair investigation.
- Personal information will be limited to those who need it. Investigation files will be access-restricted and retained according to legal, contractual, safeguarding, awarding-organisation and records-management requirements.
- Original source records, metadata and system logs must be preserved. A legal or investigation hold overrides ordinary disposal schedules until authorised release.
- Communication with staff, learners, employers and external bodies must be factual, authorised and consistent. Public or media statements require senior approval.

13. Roles and Responsibilities

Role	Core responsibilities	Evidence / assurance
Director of Contracts & Operations	Set tone; resource controls; approve material investigations and notifications; protect public funds; ensure recovery and remediation; avoid or declare conflicts.	Risk review, decision records, funder correspondence, action closure.
Quality & Compliance Lead	Own policy; maintain fraud/irregularity register; coordinate triage; review learner, funding and assessment evidence; monitor actions and wider-population checks.	Register, audit reports, investigation files, QIP, governance reporting.
Independent Governor / external adviser	Provide independent challenge or investigation where senior leaders, connected persons or normal reviewers are conflicted.	Declaration, terms of reference, report, review record.
Finance / accounts support	Verify suppliers and bank changes; maintain accounting records; reconcile payments; flag anomalies; preserve evidence and support recovery.	Invoices, approvals, call-back records, bank/accounting reconciliations.
MIS / data staff	Maintain accurate PICS/ILR records; run validation and reconciliation; record corrections; report unexplained anomalies.	PICS audit, FIS/PDSAT, occupancy reports, error and correction log.
Tutors, assessors and IQAs	Record delivery and assessment accurately; protect authenticity; refuse improper instruction; report suspected fabrication, collusion or false claims.	Registers, learner work, assessment/IQA records, concern reports.
Learner engagement and progression staff	Use accurate IAG, eligibility and employer information; verify interviews and outcomes; maintain contact and evidence trails.	IAG, contact records, employer verification, progression tracker.
Managers and budget holders	Apply approvals, conflicts and due diligence; review unusual transactions and staff evidence; escalate concerns.	Approval logs, conflict declarations, performance and purchasing records.
All staff and associates	Complete training; follow controls; keep records; protect credentials; report concerns promptly; cooperate with reviews.	Training, acknowledgements, records, statements.
Learners, employers and suppliers	Provide truthful information and evidence; disclose conflicts; report suspected improper conduct; cooperate with reasonable verification.	Declarations, contracts, correspondence and verification evidence.

14. Monitoring, Assurance and Review

Monitoring activity	Purpose	Frequency / trigger
Fraud risk assessment	Identify inherent and residual risks, controls, gaps, owners and actions.	At least annually; new contract/system; significant incident or change.
Fraud and irregularity register review	Check cases, values, timescales, notifications, recovery, themes and action closure.	Monthly operational review; quarterly leadership/governance overview.

Monitoring activity	Purpose	Frequency / trigger
Funding and learner-file assurance	Test eligibility, attendance, assessment, achievement and MS3 evidence against contract and system records.	Risk-based sampling before claims and through monthly/contract review.
Payment and supplier controls	Review bank-detail changes, duplicate invoices, unusual payments, related-party transactions and approval compliance.	At each relevant transaction; periodic reconciliation.
Gifts, hospitality and conflicts	Identify repeated, high-risk or decision-linked offers and ensure mitigation.	Event-driven declarations; quarterly register review.
Training and staff confidence	Ensure staff know red flags, reporting routes and evidence-preservation duties.	Induction; annual refresher; after incidents or material policy change.
Investigation action review	Confirm correction, recovery, disciplinary/contract action and control improvements are complete and effective.	After each case and through QIP monitoring.
Policy review	Check legislation, guidance, funder rules, awarding-organisation requirements, systems and roles remain current.	August 2027 or sooner as required.

Assurance standard

Leaders must be able to demonstrate what was checked, who checked it, what was found, what changed and whether the action reduced risk. A clean result must also be recorded; absence of reported fraud is not, by itself, evidence that controls are effective.

Appendix A: Fraud and Irregularity Red Flags

Area	Illustrative red flags
Learner records	Repeated identical handwriting or signatures; unexplained shared contact details; evidence created after the claim; inconsistent dates; missing original documents; unusual postcode or eligibility pattern.
Attendance	Perfect attendance despite contradictory contact notes; identical signing times; Teams records inconsistent with registers; regular full-day claims where learners report early finishes.
Assessment	Sudden change in writing style; identical answers; learner unable to explain work; metadata inconsistent with learner; assessment completed before teaching; unsupported assessor decisions.
Progression / MS3	Employer email domain inconsistent; employer cannot confirm learner; payslip dates/pay inconsistent; repeated employer signatures; job title not linked to evidence; outcome claimed before start.
Finance	Duplicate invoice number/amount; urgent bank-detail change; round-sum invoice without deliverables; payment just below approval threshold; personal bank account; supplier linked to staff but undeclared.
Cyber	Unexpected MFA prompt; mailbox rule; urgent executive payment request; lookalike domain; changed invoice details; supplier unwilling to verify by telephone.
Behaviour	Resistance to review; unexplained record deletion; pressure to backdate; instruction to “make the evidence fit”; secrecy beyond legitimate confidentiality; repeated bypassing of controls.

Red flags require proportionate review. They must not be used as a substitute for evidence or to make discriminatory assumptions about a learner, employee, employer or supplier.

Appendix B: Initial Triage and Evidence-Preservation Checklist

Check	Required action	Complete / evidence
Concern recorded	Record reporter, date/time, allegation, affected contracts/learners, value and known evidence.	
Immediate safety	Consider safeguarding, Prevent, exploitation, threat, self-harm or other urgent risk.	
Loss contained	Hold payment, claim, certificate or access where necessary and proportionate.	
Evidence secured	Preserve files, emails, messages, logs, devices, paper records and original system audit trails.	
Conflict checked	Confirm triage lead and investigator are not implicated or materially conflicted.	
External duties assessed	Consider funder, awarding organisation, police, bank, insurer, ICO, HMRC or other notification.	
Affected population defined	Identify whether wider sample or full review is required.	
Communication controlled	Agree authorised contacts and factual message; avoid prejudging the outcome.	
Case owner and review date	Assign owner, terms of reference, target date and interim-control review.	

Appendix C: Investigation and Corrective-Action Checklist

Stage	Minimum evidence
Terms of reference	Allegations, scope, investigator, authority, conflicts, records, interviews and reporting line.
Evidence schedule	Source, date obtained, custodian, integrity, relevance and storage location.
Financial / funding impact	Actual, potential and prevented loss; claims affected; recovery status.
Learner / qualification impact	Learners, assessments, certificates, progression and safeguarding affected.
Findings	Finding for each allegation, evidence relied upon, response considered and standard applied.
Wider review	Population tested, sampling rationale, findings and need for full review.
Notifications	Who was notified, when, by whom, facts provided and further reporting deadlines.
Corrections	System, record, claim, invoice or certificate corrected; original audit trail retained.
Sanctions / recovery	Employment, learner, supplier, civil, insurance, awarding-body or law-enforcement action.
Root cause and controls	People, process, system, culture or governance cause; action, owner, due date and effectiveness check.

Stage	Minimum evidence
Closure	Senior approval, independent review where required, reporter/witness protection and retention decision.

Appendix D: Fraud Risk Assessment Template

Field	Required entry
Risk statement	Describe who could commit what act, by what method, and who could benefit or suffer loss.
Area / process	Contract, learner journey, assessment, finance, payroll, supplier, cyber or other process.
Inherent likelihood / impact	Rate risk before controls and record rationale.
Existing controls	Specific preventative, detective and response controls with evidence location.
Control owner	Named role responsible for operating and reviewing each control.
Control effectiveness	Effective, partly effective or ineffective, supported by assurance evidence.
Residual likelihood / impact	Rate remaining risk after controls.
Further action	Action, owner, due date, resources and expected evidence.
Review trigger	Annual date, new contract/system, incident, external finding or material change.

Appendix E: Gifts and Hospitality Declaration Checklist

Check	Required information
Person and role	Recipient/offering person, organisation, role and relationship to Quack.
Offer	Description, date, location and estimated value.
Context	Current or planned procurement, recruitment, audit, assessment, claim, contract or other decision.
Decision	Accepted, declined, returned, donated or modified, with approver and rationale.
Conflict mitigation	Recusal, second review, restricted involvement or other control.
Register and review	Date recorded and any repeated-pattern or quarterly review action.

Appendix F: Version Control

Version	Date	Author / owner	Summary of change	Next review
1.0	2024	Dion Bishop	Original generic Counter Fraud Policy.	Superseded
2.1	August 2026	Dion Bishop / Quality Team	Complete rewrite for adult Skills Bootcamp, recruitment and corporate operations. Added public-funding, ILR/PICS, assessment, MS3, bribery, gifts, cyber fraud, investigation, external reporting, recovery and assurance controls.	August 2027

Reference framework

Fraud Act 2006; Bribery Act 2010 and Ministry of Justice guidance; Economic Crime and Corporate Transparency Act 2023 failure-to-prevent-fraud guidance; Criminal Finances Act 2017; Theft Act 1968; Companies Act 2006; UK GDPR and Data Protection Act 2018; Skills Bootcamp contract and funding requirements; awarding-organisation rules; Ofqual requirements; GovS 013 Counter Fraud as relevant good practice.