FRAUD PREVENTION AND RESPONSE POLICY

Honesty, accountability and proportionate prevention

Policy owner	The Directors
Approved by	The Directors
Version	2.1
Effective date	23 July 2026
Next review date	23 July 2027

Controlled document. Printed copies may be out of date.

Policy title	Fraud Prevention and Response Policy
Policy owner	The Directors
Legal entity	The Initiative Training GP Limited, company number 06204390
Applies to	Directors, employees, workers, consultants, subcontractors, agents, suppliers and other persons acting for or on behalf of Initiative Training Group
Approved by	The Directors
Effective date	23 July 2026
Review cycle	At least annually and after any material incident, legal change or significant change in business activities
Version	2.1 - replaces the Fraud Policy dated 16 July 2020
Status	Approved

This policy should be read with the Whistleblowing Policy, Anti-Bribery and Corruption Policy, our Privacy and Cookies Policy, contractual terms and conditions, financial procedures, supplier due-diligence arrangements and any applicable disciplinary or consultant management procedures.

Policy statement

Initiative Training Group has zero tolerance for fraud, attempted fraud, deliberate misrepresentation or dishonest conduct. Concerns will be handled promptly, fairly, confidentially and without retaliation against anyone who raises a genuine concern.

1.1 The Initiative Training GP Limited, trading as Initiative Training Group and Initiative Training Oracle (“ITG”), is committed to conducting business honestly, responsibly and transparently. Fraud is incompatible with those standards and will not be tolerated, whether it is intended to benefit an individual, ITG, a client or another party.

1.2 The purpose of this policy is to prevent fraud where reasonably possible, identify concerns early, provide clear reporting routes, preserve evidence, support fair investigation and ensure proportionate action is taken.

1.3 ITG will not knowingly misstate the services it has delivered, the qualifications or licences of personnel, the work completed, the time or expenses incurred, the results achieved, the risks identified, or any entitlement to payment, funding, reimbursement or other benefit.

1.4 Where ITG identifies an honest inaccuracy or error, it will correct the record promptly, inform any affected client, funding body or other relevant party where appropriate, and repay money to which it is not entitled. An honest mistake is not fraud, but concealing it or knowingly allowing it to continue may become misconduct or fraud.

1.5 Controls will be proportionate to ITG's size, structure, risk profile and operating environment. No control system is infallible, so openness, professional judgement and prompt reporting remain essential.

2.1 This policy applies to all ITG directors, employees, workers, consultants, subcontractors, agents, suppliers, business partners and any other person performing services for or on behalf of ITG. In this policy they are collectively referred to as “associated persons”.

2.2 It applies to conduct in the United Kingdom and overseas, including conduct connected with travel risk management, training, consultancy, protective security, procurement, client delivery, financial administration, marketing, tenders and the use of ITG information or assets.

2.3 Compliance with this policy may be made a contractual requirement. A failure to comply may result in disciplinary action, removal from duties, suspension of access, termination of engagement or contract, recovery action and referral to law enforcement or another competent authority.

3.1 Fraud is dishonest conduct intended to make a gain, cause a loss, expose another person to a risk of loss, or obtain a benefit to which a person or organisation is not entitled. It may involve an act, an omission, a false statement, concealment, abuse of a position of trust, collusion or the misuse of information or systems.

3.2 Fraud includes attempted fraud. The intended gain or loss does not need to occur before a concern can be investigated or action taken.

3.3 Examples include:

- creating, approving or submitting false, altered, duplicate or inflated invoices, purchase orders, expenses, timesheets or claims;
- misrepresenting qualifications, experience, vetting, security clearances, professional licences, SIA licences, insurance or right-to-work status;
- falsifying training attendance, assessment results, certificates, project records, risk assessments, incident records, operational documentation or management information;
- misrepresenting services delivered, project progress, personnel deployed, hours worked, costs incurred, risk findings or performance achieved;
- diverting payments, changing bank details dishonestly, using personal accounts improperly or manipulating supplier and client payment instructions;
- theft or unauthorised use of money, equipment, intellectual property, confidential information, client data or other assets;
- concealing a conflict of interest, accepting secret commissions, colluding with a client or supplier, or manipulating a tender or procurement process;
- phishing, impersonation, cyber-enabled fraud, unauthorised access or misuse of IT systems to obtain money, information or advantage;
- deliberately withholding information where there is a duty to disclose it, or abusing a position in which another person expects honest and responsible conduct.

3.4 An irregularity, control weakness or mistake is not automatically fraud. It must still be reported when it could cause loss, misstatement, client harm or reputational damage, or when there is uncertainty about whether the conduct was deliberate.

4.1 This policy is informed by applicable UK law and official guidance, including the Fraud Act 2006, the Theft Act 1968, the Bribery Act 2010, the Criminal Finances Act 2017, the Economic Crime and Corporate Transparency Act 2023, the Employment Rights Act 1996, the Data Protection Act 2018 and the UK General Data Protection Regulation.

4.2 The corporate offence of failure to prevent fraud under the Economic Crime and Corporate Transparency Act 2023 applies to large organisations meeting the statutory criteria. ITG adopts the underlying prevention principles proportionately as good practice, regardless of whether the statutory size threshold applies to ITG at any particular time.

4.3 This policy is not a substitute for legal advice. ITG will obtain professional advice where an allegation raises material legal, regulatory, contractual, insurance, employment or cross-border issues.

- set the tone from the top and ensure that profit, convenience or commercial pressure never justifies dishonest conduct;
- approve this policy and oversee its implementation;
- ensure that significant fraud risks are assessed and that proportionate controls are maintained;
- decide whether specialist legal, forensic, accounting, insurance, employment or investigative support is required;
- receive reports of suspected fraud and ensure that allegations involving a Director are handled independently;
- review material incidents, losses, control failures and lessons identified.

The Managing Director, or another Director nominated in writing, will act as the Fraud Policy Lead. The role includes maintaining the fraud risk assessment, coordinating reports and investigations, preserving records, monitoring remedial action and arranging appropriate communication or training. The role may be delegated for a particular case where independence or specialist expertise is required.

- apply the controls relevant to their work and do not bypass them for speed or convenience;
- verify records, approvals, qualifications, licences, expenses and deliverables where their role requires it;
- escalate concerns promptly and preserve relevant evidence;
- avoid investigating allegations themselves unless formally authorised.

- act honestly and within their authority;
- maintain accurate, complete and timely records;
- declare actual, potential or perceived conflicts of interest;
- protect ITG and client information, systems, money and property;
- challenge unusual instructions and report suspected fraud or control weaknesses promptly;
- co-operate fully and truthfully with any authorised review or investigation.

6.1 ITG will use a proportionate framework based on six principles: top-level commitment, fraud risk assessment, proportionate risk-based procedures, due diligence, communication and training, and monitoring and review.

ITG will periodically identify where fraud could occur, who might commit it, how ITG or a client could benefit or suffer loss, what controls exist, and what further action is reasonably required. The assessment will consider internal and external fraud, associated persons, overseas operations, remote working, subcontracting, digital systems, client requirements and payment processes.

- clear authority limits and documented approval for expenditure, commitments, credit notes, refunds and payments;

- separation of initiation, approval and payment duties where practical, with compensating review where the size of the business makes full separation impracticable;
- independent verification of new suppliers and any request to change bank details, using a trusted contact method rather than the contact details supplied in the change request;
- supporting evidence for invoices, expenses, timesheets, subcontractor charges and client billing;
- regular reconciliation and review of bank, accounting, debtor, creditor and expense records;
- prompt challenge of duplicate, unusual, urgent, split or round-sum transactions.

- written scopes, proposals, contracts or task instructions that define deliverables, responsibilities and payment terms;
- accurate recording of work performed, personnel used, travel undertaken, hours, expenses, decisions, findings and client approvals;
- verification of identity, competence, references, qualifications, vetting, insurance and licences proportionate to the role and risk;
- quality review of significant risk assessments, operational instructions, training records, reports and client deliverables;
- controlled issue, amendment and retention of certificates, reports, policies and other formal documents;
- appropriate access controls, multi-factor authentication, secure backups and prompt removal of access when an engagement ends.

Before appointing a higher-risk consultant, subcontractor, supplier, agent or partner, ITG will conduct and record proportionate due diligence. This may include identity, ownership, capability, references, financial standing, licences, insurance, conflicts, sanctions exposure, adverse information, payment arrangements and the commercial rationale for the appointment.

Contracts should contain appropriate requirements on honesty, records, audit or information rights, conflicts, confidentiality, compliance with law, fraud reporting, co-operation with investigations and termination for misconduct.

Actual, potential or perceived conflicts of interest must be declared promptly. Remuneration, targets, commissions, referral arrangements and project pressures must not encourage misstatement, concealment or the acceptance of work that cannot be delivered lawfully or competently.

The presence of a red flag does not prove fraud. It requires proportionate checking and, where appropriate, escalation. Examples include:

- unexpected, urgent or secret payment instructions, particularly where normal approval routes are bypassed;
- a request to pay a different bank account, personal account, unfamiliar jurisdiction or unrelated third party;
- altered, duplicate, vague or unsupported invoices, expenses, timesheets, qualifications, licences or certificates;
- unexplained differences between work records, client information, accounting records and actual delivery;
- pressure to sign, approve or certify something known to be incomplete, inaccurate or unverified;
- resistance to due diligence, audit, quality assurance, evidence requests or normal contractual terms;
- undisclosed relationships or conflicts involving a supplier, client, candidate or decision-maker;
- unusual pricing, commissions, discounts, refunds, subcontracting, cash transactions or split payments;
- emails, websites, invoices or messages that imitate a known person or organisation, contain changed contact details, or request credentials or payment;
- deletion, concealment, backdating or unexplained alteration of records after a query has been raised.

8.1 Anyone who knows or reasonably suspects that fraud, attempted fraud or a serious control failure has occurred must report it promptly to the Fraud Policy Lead or any Director. A concern may be raised verbally or in writing. Enough information should be provided to explain what happened, who may be involved, when it occurred, the records or systems affected, and any immediate risk.

8.2 Where the concern involves the person who would normally receive the report, it must be raised with another Director. If no internal route is appropriate, the reporter may raise the matter with ITG's legal adviser, accountant, insurer, a prescribed external body or law enforcement, as appropriate.

8.3 Reports will be treated confidentially and information will be shared only with those who need it. Anonymous reports will be considered, although anonymity can limit the ability to clarify evidence or provide feedback.

8.4 ITG will not tolerate dismissal, detriment, victimisation or retaliation against a person who raises a genuine concern or participates honestly in an investigation. A report that is not substantiated is not, by itself, malicious or improper.

8.5 Knowingly making a false allegation, fabricating evidence or using the process to harm another person may itself result in action.

> **Do not investigate the matter yourself**
>
> Do not confront the suspected person, search systems without authority, alter records, delete messages, discuss the allegation widely or promise a particular outcome. Preserve what you lawfully hold and report it promptly.

9.1 The recipient of a report will acknowledge it where possible, create a secure record and conduct an initial assessment. Immediate priorities are to protect people, stop further loss, secure evidence, preserve legal privilege where relevant, protect client operations and avoid prejudicing any criminal, regulatory or employment process.

9.2 Depending on the circumstances, immediate action may include:

- suspending a payment, transaction, system account, document issue or operational activity;
- contacting a bank, payment provider, insurer, client or system provider through a trusted channel;
- preserving emails, messages, files, logs, devices, access records, financial records and physical documents;
- restricting access or temporarily reassigning duties without treating the measure as a finding of guilt;
- obtaining legal, forensic, accounting, employment, data protection or security advice;
- notifying the police or another competent authority where delay could increase harm or compromise evidence.

9.3 The Directors will decide who should investigate. The investigator must have appropriate competence and independence. A matter involving a Director, material client interest or significant conflict will normally be referred to an external adviser or otherwise managed independently.

9.4 The investigation will be proportionate and documented. It may define the allegations, scope, evidence, interview plan, confidentiality arrangements, reporting line, legal issues, decision-making responsibility and expected timescale. The subject of an allegation will be treated fairly and given an appropriate opportunity to respond before conclusions are reached, unless doing so would create a serious risk to people, evidence or an external investigation.

9.5 The standard used for an internal finding will normally be the balance of probabilities, unless a contract, law or procedure requires otherwise. Internal findings do not determine criminal guilt.

10.1 Where wrongdoing or a control failure is established, ITG may take one or more of the following actions:

- disciplinary action, removal from duties or termination of employment, engagement, agency, supplier or subcontractor arrangements;
- recovery of money, property, information or other losses, including civil proceedings where proportionate;
- correction of records, invoices, reports, certificates, client communications, accounts or regulatory submissions;
- notification to affected clients, insurers, banks, auditors, professional bodies, awarding bodies, regulators, contracting authorities or funders where required or appropriate;
- reporting to the police or the national Report Fraud service, or to another relevant enforcement body;
- improvements to controls, contracts, systems, supervision, training, due diligence or quality assurance.

10.2 Decisions about reporting, disclosure and recovery will consider legal duties, contractual requirements, public interest, client safety, preservation of evidence, insurance conditions, data protection and the risk of further harm. ITG will not enter into an agreement intended to conceal criminal conduct or prevent a legally protected disclosure.

10.3 After a material incident, the Directors will review root causes, warning signs, control performance, lessons identified and completion of corrective actions.

11.1 Fraud reports and investigation records will be handled on a strict need-to-know basis and stored securely. Access will be limited to authorised persons with a legitimate role in receiving, assessing, investigating, advising on or deciding the matter.

11.2 Personal information will be processed lawfully, fairly and proportionately under applicable data protection law. ITG will collect only information reasonably required, take care with special category and criminal offence data, keep records accurate, protect them against unauthorised access and retain them only for as long as necessary under the applicable retention arrangements or legal requirements.

11.3 Confidentiality cannot be guaranteed absolutely. Information may need to be disclosed to the subject of an allegation, a client, insurer, regulator, professional adviser, court or law-enforcement body. Where possible, the reporter will be informed before their identity is disclosed, unless this would be unlawful, impracticable or prejudicial.

11.4 No person may destroy, conceal, falsify, backdate or improperly remove a record relevant to a suspected fraud, investigation, dispute, insurance claim, audit or legal process.

12.1 This policy will be made available to persons working for or on behalf of ITG. Its requirements will be communicated at the start of relevant employment, consultancy, subcontracting, supplier or partnership arrangements and reinforced according to risk.

12.2 Training or briefing will be proportionate to role and exposure. Higher-risk roles may receive specific guidance on payment fraud, procurement, expenses, document integrity, cyber-enabled fraud, conflicts, due diligence, whistleblowing and the preservation of evidence.

12.3 Suppliers, consultants, subcontractors and business partners may be required to confirm compliance and to communicate equivalent expectations to persons they use to deliver ITG work.

13.1 The Fraud Policy Lead will monitor reports, incidents, near misses, control exceptions, due-diligence findings and relevant changes in law, guidance, technology and ITG operations.

13.2 The Directors will review this policy at least annually and sooner following a significant fraud concern, material control failure, change in business activity, corporate structure, client requirement or legal framework.

13.3 The review will consider whether the fraud risk assessment remains current, whether controls are proportionate and operating effectively, whether reports are handled properly, and whether lessons and remedial actions have been completed.

13.4 Amendments must be approved by the Directors and recorded through version control.

Protect and pause	Deal first with any immediate threat. Where authorised, hold the relevant payment, transaction, document issue, access or activity.	**Preserve**	Keep original emails, messages, invoices, logs, files, notes and devices. Do not alter or delete them.
Report	Contact the Fraud Policy Lead or another Director promptly. Use an alternative route if the concern involves that person.	**Record**	Write down the facts, dates, people, systems and documents involved. Separate what you know from what you suspect.
Limit discussion	Share the concern only with those who need to know. Do not confront the suspected person.	**Follow instructions**	Co-operate with authorised steps and preserve confidentiality.

Area	Illustrative example
Travel risk management	A consultant copies an old assessment, removes caveats and presents it as current work without conducting the agreed research or itinerary analysis.
Training	Attendance or assessment records are altered to show that a learner completed training, or a certificate is issued where the required standard was not met.
Protective security	A subcontractor claims to hold a current licence, vetting status or insurance that has expired or never existed.
Billing	Time, travel, accommodation, subsistence or subcontractor costs are inflated, duplicated or charged to more than one client.
Procurement	A person hides a relationship with a supplier and steers work to that supplier in return for a personal benefit or undisclosed commission.
Payment diversion	A criminal impersonates a Director or supplier and requests an urgent change of bank details. The request is paid without independent verification.
Client reporting	An incident, delay, control failure or material risk finding is deliberately concealed to protect revenue, reputation or contract renewal.

Approved by the Directors of Initiative Training Group on 23 July 2026. This version replaces the Fraud Policy dated 16 July 2020.