QAHE Limited Counter Fraud and Error Policy

Prepared by: Chief Governance & Transformation Officer

Prepared for: Board of Directors

Date: February 2026

Issue: 1

Version Control

Document Information	
VO1	Original draft of the Counter Fraud and Error Policy for Board approval.

Document Approval		
Board	**Approval**	**Viewed / Comments / Date**
QAHE Board of Directors	Approved	12 February 2026
		Approved

Revision History			
Version	**Issue Date**	**Author**	**Description of Change**
VO1	February 2026	Chief Governance & Transformation Officer	Policy based on the QA Group Counter Fraud and Error Policy. Policy amended for the structure of QAHE and for approval by the Board of Directors.

Contents

1. Introduction

QAHE Limited ("QAHE") is a part of the QA Group. As part of a wider group structure, we operate a comprehensive framework of policies designed to safeguard our institution and uphold the highest standards of integrity, this is our Counter Fraud Framework (the "Framework").

Across the QA Group, we maintain and regularly update a suite of policies that work together as a framework which enables us to operate in a manner which is consistent, strengthens our resilience to fraudulent activity, and supports a robust culture of accountability and transparency.

QAHE operates a comprehensive Framework designed to prevent, detect, and respond to fraud. This Framework includes risk identification, proportionate controls, governance oversight, a formal fraud risk register, and a structured response plan. The Framework explicitly addresses risks relating to public funds, including student finance, regulatory reporting, and funding eligibility.

Our Framework policies are:

- Corporate Crimes Policy
- Counter Fraud and Error Policy
- Sanctions Policy
- Anti-Facilitation of Tax Evasion Policy
- Anti-Money Laundering Policy
- Conflict of Interest Policy
- Anti-Bribery Policy
- Whistleblowing Policy
- Gifts and Hospitality Policy
- Fraud Response Plan
- Financial Regulations
- Delegation of Authority

Each policy sets out roles, responsibilities, and how the QA Group works together to ensure veracity around this Framework. The Framework policies are underpinned by the Fraud Response Plan.

QAHE is committed to the proper use of our finances and resources and endeavours to ensure transparent and accountable working practices.

Providing best value and ensuring that decisions are taken transparently and clearly, are key principles for QAHE and we are committed to maximising our resources for the benefit of our staff and student community. As an institution and as individuals, we have a duty to ensure that all of our dealings are conducted to the highest standards of integrity.

This policy supports the integrity and lawful use of public funds in line with regulatory expectations, including OfS Condition E8 and the OfS Public Interest Governance Principles and forms part of QAHE's "reasonable procedures" to prevent fraud. This policy operates alongside key governing documents, including the Delegation of Authority and Financial Regulations, as part of QAHE's overall governance framework.

2. Scope

In accordance with our Framework, the Counter Fraud and Error Policy (the "Policy") applies to all employees of QAHE, students, and those who we may outsource our services to or who may perform services on behalf of QAHE including temporary workers, consultants, contractors, agents and subsidiaries ("associated persons") within the UK and overseas and seeks to ensure that:

- our business is run with the highest legal and ethical standards, and will not be party to fraud, corruption, theft and other activities involving dishonesty, in all its forms; and
- the appropriate disposition of any material errors or omissions impacting QAHE's financial statements and disclosures.

All QAHE employees must work together to ensure QAHE remains untainted by fraud and that our financial statements are properly adjusted to reflect the impact of the identified errors or omissions along with all applicable disclosures.

This Policy is a crucial element of that effort. It has the full support of the Board of Directors. It sets out the steps we all must take to prevent fraud facilitation in our business and to comply with relevant legislation. We reserve the right to amend it at any time.

3. Application and Governance

QAHE has a zero-tolerance approach to non-compliance with this Policy. Failure to comply puts both you and QAHE at risk. Any violation or attempted violation of this Policy may result in appropriate action. Violations may also result in disciplinary action up to, and including, summary dismissal or termination of a supplier contract.

4. What is Fraud and how does it affect QA?

Fraud may be described as:

(i) wrongful or criminal deception intended to result in financial or personal gain; or

(ii) a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities.

All these are clearly applicable to the education, learning, training and development sector in which QAHE operates on a global basis.

5. Examples of Fraud

Examples of fraud QAHE may be susceptible to, but are not limited to:

- Fraud relating to cash, physical assets or confidential information
- Procurement fraud
- Payroll fraud
- Financial accounting fraud
- Fraudulent expense claims
- Reference, qualification and related employment fraud
- Recruitment and appointment fraud
- Bribery and corruption
- Academic fraud including, but not limited to immigration, admissions, examinations and awards

- Fraud relating to public funds and regulatory reporting, including;
  - Student funding eligibility fraud (for example misrepresentation of identity, residency, or qualifications)
- Student Loans Company (SLC) funding irregularities or incorrect claims
  - Attendance and engagement manipulation
  - Retention, progression, or completion misreporting
  - Inaccurate or misleading data returns to partners, the Office for Students (OfS), or other regulators.

6. Failure to Prevent Fraud

6.1. What is the Failure to Prevent Fraud?

Under the Economic Crime and Corporate Transparency Act 2023 ("ECCTA") a new corporate Offence, Failure to Prevent Fraud, has been created. Under this new offence QAHE may be held criminally liable if it fails to prevent fraud committed by persons associated with the company. This applies to all employees in large organisations.

Under the ECCTA, QAHE is held accountable for fraud committed by associated persons unless it can demonstrate that reasonable procedures were in place to prevent such misconduct. Reasonable procedures may include robust internal controls, regular audits, mandatory staff training, etc. These measures need to ensure that employees understand their responsibilities, enable early detection of suspicious activity, and help the company manage legal and reputational risks, including the prevention, detection and stopping of fraud.

6.2. What procedures does QAHE have in place?

QAHE conducts comprehensive risk assessments, maintains and updates policies and internal controls, and provides relevant mandatory training to ensure all employees understand what constitutes fraud and how to prevent it. Executive Board and the Audit and Risk Committee oversee these measures, ensuring that employees are supported and held accountable.

6.3. How does this offence affect me?

All employees have a responsibility to prevent, identify, and report suspicious or fraudulent behaviour. Misconduct anywhere in QAHE can expose QAHE to legal risk.

6.4. Reporting Concerns

Employees are encouraged to raise concerns through internal reporting channels. Reports can be made confidentially or anonymously via the whistleblowing email or confidential helpline. Protections are in place under the ECCTA and other legislation to prevent retaliation against whistleblowers. Employees should escalate any suspicious activity promptly, see 11.1 Fraud below for details.

6.5. Consequences of Failure to Prevent Fraud

Failure to prevent fraud can result in serious consequences for both the company and individuals. This may include prosecution, substantial fines, and reputational damage. Employees who fail to comply with reporting obligations or who engage in fraudulent behaviour may also face disciplinary action, including dismissal and potential legal proceedings.

7. Monitoring

QAHE monitors compliance with this Policy through a combination of risk management

processes, internal controls, and assurance activities designed to detect, prevent and respond to (including stopping) fraud and the inappropriate use of public funds (including Student Loans Company funding, OfS-related funding and partner funding flows).

. This includes periodic review of:

- financial controls and transaction monitoring;
- tax compliance and reporting processes;
- data integrity and the accuracy of data used in funding claims, student-related returns, and regulatory submissions;
- regulatory reporting processes (including student-related data returns, tuition fee records, and funding claims, whether to partner universities or other regulatory bodies including the OfS and SLC);
- third-party arrangements, including agents, contractors, and suppliers.

Monitoring activities are designed to detect and prevent fraud, including where this could impact public funding or regulatory reporting. QAHE maintains a track record of compliance in its use of public funds and will promptly investigate and address any identified irregularities, including meeting any reporting or repayment obligations where required.

7.1. Risk Management

QAHE aims to ensure its anti-fraud procedures are proportionate to the risks it faces. Fraud risk management forms a core component of QAHE's governance and internal control framework.

We have undertaken an assessment of the risk of QAHE being exposed to fraud. This Policy has been developed in response to that assessment. Risk assessments are reviewed periodically and updated to reflect changes in operations, regulatory expectations, and emerging risks.

We have identified certain aspects of our operations that present a higher inherent risk of exposure to fraud facilitation. These include:

- engagement of contractors, consultants, and third parties acting on behalf of QAHE;
- commission-based arrangements, including sales staff and student recruitment agents;
- relationships with agents linked to student recruitment and associated financial flows;
- high volumes of supplier and customer transactions requiring appropriate due diligence;
- international operations, including cross-border payments and recruitment activity.

Appropriate controls, including due diligence, contractual safeguards, and financial oversight, are applied to mitigate these risks.

7.2. Fraud Risk Register

QAHE maintains a formal Fraud Risk Register to identify, assess, and manage fraud and error risks across QAHE.

Ownership: The Fraud Risk Register is owned by the Chief Financial Officer.

Governance: It is reviewed regularly and formally reported to the Audit and Risk Committee.

Integration: It is aligned to the Strategic Risk Register and informs the internal audit programme.

Scope: It includes risks relating to financial crime, operational fraud, cyber fraud, and public funding risks.

Review: Risks and controls are reviewed periodically to reflect emerging threats, regulatory changes, and operational developments.

This structured approach supports QAHE's compliance with regulatory expectations and the ECCTA.

7.3. Assurance

QAHE operates this structured assurance Framework to evaluate the effectiveness of our fraud prevention controls. This includes:

- Internal audit reviews aligned to key fraud risks
- Data validation and reconciliation processes, particularly relating to student and financial data
- Compliance monitoring across key business processes
- Periodic reporting of fraud risk metrics, incidents, and control effectiveness to senior management and the Audit and Risk Committee
- This Framework ensures that controls are operating effectively and supports continuous improvement.

7.4. Mandatory Training

Completion of mandatory training is monitored by the People Team and reported to the Executive Board to ensure compliance and to the Audit and Risk Committee for oversight and assurance. Non-completion is followed up and may be escalated in line with internal procedures.

Training content is reviewed periodically to ensure it remains relevant, proportionate, and aligned with current legal and regulatory requirements and aligned to identified fraud risks and is supported by ongoing assurance activities, including monitoring completion rates, effectiveness assessments, and internal audit validation. Individuals with responsibilities under the Framework are appropriately skilled and supported through training and governance structures, and additional or role-specific training may be provided where higher corporate crime risks are identified.

7.5. Governance and Oversight

Overall accountability for this Policy and QAHE's Counter Fraud Framework sits with the Board of Directors.

The Chief Financial Officer is the executive owner of this Policy, supported by the Head of Legal.

The Executive Board is responsible for the implementation, operation, and periodic review of this Policy and associated controls, ensuring that fraud risks are effectively identified, assessed,

and managed in line with QAHE's Risk and Opportunity Management Framework.

The Audit and Risk Committee provide independent oversight of QAHE's arrangements for the prevention, detection, and management of fraud risks. The Audit and Risk Committee reviews risk exposures, controls effectiveness and assurance activity and must be satisfied that appropriate systems of internal control are in place and operating effectively.

The Board of Directors retains ultimate responsibility for ensuring that effective governance arrangements are in place and that QAHE complies with its legal and regulatory obligations, including those relating to fraud risks.

Independent assurance over the effectiveness of controls is provided through internal audit or equivalent review activity, with findings reported to the Audit and Risk Committee.

Fraud risk management forms a core component of QAHE's governance and internal control framework.

8. Record

It is essential that we keep full and accurate records of all our financial dealings as transparency is vital. False or misleading records could be very damaging to QAHE.

9. Cyber Security

QA Group's Security Operations team are responsible for security monitoring and managing detected threats to security as detailed in the QA Group Security Management Policy which can be found on our Intranet under "Policies". To mitigate the risks associated with cyber errors and fraud, QAHE deploys advanced threat detection and prevention systems to identify and block malicious activities in real-time. Multi-factor authentication and strong password policies are enforced to ensure secure access to systems and data. Network segmentation and encryption of sensitive data both in transit and at rest protect against unauthorised access and data breaches. Continuous monitoring and logging of all network activities enable prompt detection and response to suspicious behaviours. Periodic audits and assessments (including pen testing) of the cyber controls are crucial to ensure their effectiveness and to adapt to the evolving threat landscape. By implementing these cyber controls, QAHE can significantly reduce the likelihood and impact of cyber errors and fraud.

10. Your Responsibility

Everyone in QAHE is responsible for:

- reading and being aware of the contents of this Policy
- complying with this Policy and any related policies, e.g. QAHE's Whistleblowing Policy, QAHE's Corporate Criminal Offence, Tax Evasion Policy and QAHE's Anti Bribery Policy; and
- reporting cases where you know, or have a reasonable suspicion, that fraud has occurred or is likely to occur.

11. What to do if you suspect something is wrong

Each of us has a responsibility to speak out if we discover anything corrupt or otherwise improper occurring in relation to our business. We cannot maintain our integrity or comply with our various obligations unless we do this.

11.1. Fraud

If you discover or suspect that fraud has been facilitated or may be facilitated, whether by:

- another staff member
- a third party who represents us
- one of our suppliers or competitors
- anyone else—perhaps a client

You must follow our Whistleblowing Policy which can be found on the People Hub on the Policies & Forms Page. You can do this anonymously and you must make your report as soon as reasonably practicable. You may be required to explain any delays. You must report this promptly so that QAHE can take action to investigate and, where necessary, prevent further or ongoing fraud.

For students there are a variety of ways in which concerns can be raised, depending on the nature of the concern, however, "Your SafeSpace" allows for anonymous reporting where students can raise their concerns directly – Your Safe Space: Report + Support – Fill out form

11.2. Error

Any correction of errors identified must be communicated, via email, to the Chief Financial Officer clearly describing the error, its type, and its value. The disposition of the error shall be documented and approved by the Chief Financial Officer in consultation with the Group Controller.

11.3. Cyber Incident

All employees must report actual or suspected information security incidents, breaches and weaknesses to the IT Service Desk in a timely manner using any of the available channels in line with our Security Incident Management Policy, which can be found on our Intranet under Policies.

All significant information security incidents related to Finance and Accounting must be investigated and reported. Records of security incidents must be maintained, and potential evidence secured to aid in any future investigation.

12. Training

QAHE promotes a culture of integrity through regular communication and awareness activities, ensuring that all staff understand their responsibilities under this policy.

Mandatory training requirements, including monitoring and escalation of non-completion, are set out in Section 7.4. Training programmes support staff in understanding their responsibilities to prevent, detect and report fraud and risks relating to public funds.

13. Requests for information

Any requests for information concerning QAHE's information technology infrastructure, or financial data by an authorised law enforcement agency shall be directed to the Chief Financial Officer who will liaise with QA's Group General Counsel.

In the event that QAHE is notified or anticipates litigation or discovery concerning an employee, supplier, business area, or engagement, regarding fraud or other material business issues, the Chief Financial Officer will work with the appropriate employees to ensure that the appropriate retention of records occurs.

If it is found that an employee knowingly destroyed electronic records related to litigation, disciplinary action will be taken against the employee that may include termination, and such employee will likely be subject to civil and / or criminal penalties.

14. Review

This Policy will be reviewed every three years or sooner if required to ensure it remains accurate, effective, and aligned with legislation, regulatory, and institutional changes.

The policy owner is responsible for initiating and coordinating the review of this Policy in line with the Policy Framework.


POWERING
POTENTIAL