Whistleblowing Policy

Document Control		
Document Number:	AIQ-038	**Effective from**: 01-08-2026
Linked Regulatory Requirements:	General Data Protection Regulation (GDPR) – Article 5 (1)	
Version Number and Date:	v1.0, 09-07-2026	**Review date:** 09-07-2026
Date of Next Review:	02-11-2026	**Classification Level:** Public/General

Approval Level: High impact

Approved by: Executives

Date version approved: 09-07-2026

Version Number	Date	Changes
v0.1	11-06-26	Document created
v1.0	09-07-26	Document approved

Table of Contents

1. Policy principles

Aligned to our strategy to ensure we set and maintain the highest standards of compliance and risk management, this policy outlines Active IQ's approach to Whistleblowing.

Active IQ is committed to prioritising the safety and wellbeing of our colleagues whilst maintaining high standards of integrity and conduct. Our employment practices and stakeholder relationships enable us to foster an environment that is collaborative and free of malpractice or corruption.

Active IQ also aim to support its customers, contractors and third parties in raising concerns about the organisation or its colleagues.

2. Introduction

This policy outlines Active IQ's approach to handling and responding to whistleblowing disclosures, including guidance on how to raise a disclosure to Active IQ and a summary of the protections provided to whistleblowers.

Active IQ is not a Prescribed Body, and we cannot offer protection of employment rights to persons other than Active IQ colleagues.

We encourage individuals to seek independent advice in relation to their rights when whistleblowing. Please see relevant gov.uk guidance for more information.

2.1. Purpose

The purpose of this policy is to enable our centres, customers and third parties raise relevant disclosures without fear of victimisation or unfair treatment.

We respect the right of persons other than Active IQ colleagues to raise whistleblowing disclosures and recognise the importance of doing so in the protection of the public interest. To support the protection of external workers' employment rights, external parties should raise their concerns to a Prescribed Person or Body. Please see the gov.uk list of prescribed people and bodies for further guidance.

Active IQ respects the legal jurisdictions of all countries in which it operates. As such, this policy extends to all Active IQ's dealings and transactions in all countries in which it or its consultants, partners, stakeholders, and associates operate.

2.2. Scope

This policy applies to all instances where an Active IQ colleague, contractor or other third party seek to make a whistleblowing declaration in relation to the organisation, its colleagues, or its subsidiaries.

It covers any concerns about suspected wrongdoing, misconduct or violations of organisational policies including but not limited to corporate fraud, corruption, fraud or bribery. Financial mismanagement or misuse of resources. Breaches of legal, regulatory or ethical obligations. Including failure to disclose personal financial or family interests which could influence a favourable outcome.

2.3. Responsibilities/duties

All Active IQ colleagues, including apprentices, trainees, and contracted workers, must follow this policy when making a whistleblowing declaration.

Where a declaration is escalated, the responsible manager will handle and respond to the declaration.

2.4. Definitions

Word/Acronym	Definition
ARIC	Audit, Risk and Investment Committee
Colleague	Any individual employed by Active IQ
Corporate Fraud	For the purpose of this policy corporate fraud refers to deliberate, dishonest or deceptive acts carried out by an individual or group within or connected to an organisation, with the intent to secure an unlawful or unfair advantage, misled stakeholders, or cause financial or reputational harm
CRO	Chief Regulatory Officer
GDPR	General Data Protection Regulation
JCQ	Joint Council for Qualifications
PIDA	Public Interest Disclosure Act 1998

QMS	Quality Management System

2.5. Location

This policy is available externally at Active IQ Website.

3. Process

3.1. What we consider to be “Whistleblowing”

Whistleblowing is a term used when someone reports information related to bad practice, corruption, malpractice, or maladministration. Examples of whistleblowing disclosure include, but are not limited to:

- a criminal offence.
- a failure to comply with legal obligations.
- a failure to adhere to regulation and/or mandatory documentation.
- misappropriation of funds, including financial malpractice.
- any instance where an individual (including an employee of Active IQ) has committed malpractice or maladministration.
- any action intended to confuse or deceive, particularly but not exclusively
- relating to actions which has, or may have, resulted in personal and/or
- financial gain. covers corporate fraud
- health, safety, or environmental risks.
- failure to disclose a conflict of interest.
- an allegation of sexual harassment.
- concealment of information relating to any of the above.

3.2. Making a whistleblowing disclosure

When making a whistleblowing disclosure, concerns should normally be raised with the learner’s own centre in the first instance where appropriate, however, where the concern relates to the integrity, security or validity of assessments, or qualifications the centre must escalate and inform Active IQ promptly in line with the established reporting procedures.

If the concern involves a conflict of interest, such as an undisclosed personal financial relationship affecting a decision, the disclosure should clearly describe the situation and any parties involved. For further information please see the Conflicts of Interest Policy.

3.2.1. Disclosures that relate to our external stakeholders, including those relating to centres, customers, and contractors.

If an allegation relates to an external party for example, not employed by Active IQ, then the matter will be handled through our Provider Assurance team in accordance with Mandatory policies and fees | Active IQ . Please note, we may but are not obliged to accept a disclosure about a third party where we believe it is reasonable for the disclosure to be made directly to that party by the individual themselves.

3.3. Information we will need regarding disclosures in all cases.

We require as much information as possible in relation to disclosures, for example the details of the alleged incident, including dates and times and the names of the individuals involved.

We will need to understand whether other persons (such as other staff, learners, centres and/or Organisations) may have been affected by the incident, as we may be required to inform relevant external parties, such as the police, funding, and regulatory agencies and/or our regulators.

3.4. Protection and misuse under this policy

The policy offers protection to our colleagues and any workers who disclose relevant information, including allegations of sexual harassment, if they believe that disclosure:

- is made in good faith
- demonstrates that corruption, bad practice, or wrongdoing has happened
- is highly likely to have happened or is likely to happen
- is disclosed to an appropriate person.

Misuse of this policy, including disclosures that are demonstrably malicious or otherwise ill-intended, will be treated seriously and may lead to imposition of sanctions where relevant.

Matters raised in good faith which are subsequently realised to be untrue or unfounded will continue to be treated as made in good faith.

3.5. Anonymous disclosures

Active IQ may consider anonymous disclosures at the discretion of a member of the Executive team. The following will be considered when deciding whether Active IQ will consider an anonymous disclosure:

- that a qualifying disclosure was made
- the disclosure was made in the correct way to be protected by the law
- that there is a causal link between making the disclosure and the treatment received there after whether it be detriment or dismissal.

Note: Further information can be found in the (The Public Interest Disclosure Act 1998) https://www.legislation.gov.uk/ukpga/1998/23/section/1

In all instances, we strongly advise that consideration is given to making the disclosure on a named and confidential basis under the protection of this policy. Where a whistleblower requests confidentiality, Active IQ will make every effort to protect their identity.

Anonymous disclosures are more difficult to investigate and corroborate (as there is no named individual to gain further information from where required) and anonymous allegations may appear less credible.

If an anonymous disclosure is accepted by a member of the Executive team, we will investigate, providing we have enough information. If there is not sufficient information to investigate, we may log the allegation internally and may use it for future reference where appropriate.

3.6. Disclosures which are not protected

If you have been involved in the wrongdoing, making a disclosure will not protect you from any repercussions.

If you are not an employee of Active IQ, and make a disclosure in an unreasonable manner, we hold the right to treat your disclosure as vexatious.

3.7. Confidentiality

Where asked to do so, we will always endeavour to keep the identity of the individual raising a disclosure under this policy confidential. We may need to access confidential information when we consider a disclosure. We will ensure that such information is kept secure and only used for the purposes of an investigation and in line with relevant legislation.

By law and regulation, we may need to release disclosures including but not limited to:

- the police, fraud prevention agencies or other law enforcement agencies (to investigate or prevent crime, including fraud)
- the courts (in connection with any court proceedings)
- another person to whom we're required by law to disclose your identity
- relevant regulators (such as, the regulator(s) who are responsible for the standards of our qualifications and products).

3.8. Responding to a whistleblowing disclosure

What we will do when we receive a whistleblowing disclosure

The receiving manager will:

- Acknowledge receipt of the notification. If your disclosure is made by phone or in person, acknowledgement will be at the time of the call or discussion. If you made your disclosure in writing, we would acknowledge in writing (which may include by email), normally **within five working days** of receipt of the disclosure.
- Conduct an initial review of the disclosure and any additional evidence and confirm the name of staff member who will be handling the disclosure.

The initial review will include all reasonable actions required to investigate the claims made in the disclosure. This initial review period will usually be complete within **10 working days** of receipt of the notification.

Following the initial review, a determination will be made by the reviewing manager as to whether the disclosure will be accepted or rejected. If the disclosure is to be rejected this will be escalated to a Head of Department, Director or Executive to confirm this decision. Prior to making this determination, you may be asked for more evidence or information. In this case, you will be informed of any potential impact on timescales. In the main (unless the case is complex or, for example, requires significant external contact), the timescale to fully review a disclosure and decide should not normally be longer than **20 working days**.

3.9. When a disclosure is accepted

- If a disclosure about a staff member is accepted, the reviewing manager will, subject to information-sharing restrictions, inform them of the allegations as soon as possible.
- The accused member of staff should be treated fairly and honestly and supported with concerns raised against them by their line manager
- Be kept informed of the progress of and outcomes of the investigation.
- If suspended be kept up to date about events.

3.10. Escalation of cases

In some cases, such as those involving significant or complex concerns, we may need to escalate the review internally to ensure it is considered at a senior level. Where this happens, it may take longer than our standard 20 working day timeframe to complete the review. If there is any change to the timescale, we will keep you informed and provide an updated response date.

If required, we will follow appropriate regulatory or reporting requirements in line with our organisational obligations.

We will aim to maintain confidentiality throughout the process. However, to carry out a thorough and fair review, it may be necessary to share relevant information with appropriate parties. Where this is the case, we will ensure this is handled appropriately and only shared as needed.

Once the review has been completed, we will provide you with the outcome and a summary of our findings, usually via email, within five working days.

The summary:

- will not provide the granular elements of the review, but will provide details of any investigation or outcomes
- will provide sufficient information relating to our actions and decisions
- The review decision is final and there is no right of appeal against the decision. (For further confidential advice the following link is provided: https://protect-advice.org.uk/

However, if the decision is based on factual inaccuracy or omission, you may then have the right to raise these concerns by raising them with the investigating manager.

3.11. Malicious disclosures

If a disclosure has been raised maliciously or you know to be untrue your behaviour may be addressed through the appropriate Active IQ policies.

3.12. Non-whistleblowing concerns

Concerns that are not related to whistleblowing such as bullying, harassment, complaints, or grievances should normally be raised directly with your centre or organisation in the first instance, as they are best placed to address these matters.

If you feel unable to raise the issue with your centre, or if the matter has not been resolved, you can contact us for further advice or support.

3.13. Making a disclosure to the media

A disclosure to the press or publishing on social media must not take place, this may result in non-anonymity or legal protection for the whistleblower.

3.14. How to contact us

If you have any queries about the contents of the policy, please contact our support team on:

E: csteam@activeiq.co.uk

T: +44(0)1480 467 950
T: +44(0) 845 688 1278

4. Initial Equality Impact Assessment

An Initial Equality Impact Assessment has been completed for this policy, and no concerns were raised.

5. References to associated documents

- Anti-Bribery and Corruption Policy
- Conflict of Interest Policy
- Maladministration and Malpractice Policy

6. Implementation and dissemination

The policy will be implemented immediately upon approval. An external copy will be available on Active IQ website

7. Monitoring arrangements

Should an allegation be received by Active IQ that relates to an external party, such as an individual not employed by Active IQ, the matter will be handled through the Provider Assurance team. Additionally, all whistleblowing cases will be managed through a secure platform, which will restrict access to confidential information and ensure the anonymity of the whistleblower.

Active IQ operates in line with this policy and maintains appropriate governance arrangements to ensure ongoing compliance.

8. Data retention

Data must be stored for the shortest time possible. Or as set out in article 5(1) (d) GDPR, personal data shall be kept no longer than is necessary for the purposes for which the personal data are processed.

Personal data processed by a whistle blowing disclosure should be deleted, promptly and usually within two months of completion of the investigation of the facts alleged in the report. Non cases can be closed immediately, while serious misconduct investigations can take years.