Whistleblowing Policy

1. Policy Statement

JC Training & Consultancy Ltd is committed to operating with integrity, transparency, and accountability in all aspects of its work. The organisation recognises that individuals working within or alongside it may, at times, become aware of concerns relating to malpractice, wrongdoing, or serious organisational risk that cannot appropriately be addressed through normal reporting routes.

This policy provides a structured mechanism for raising such concerns in the public interest. It is designed to ensure that individuals feel confident to speak up without fear of retaliation or disadvantage, and that concerns are dealt with promptly, fairly, and in a proportionate manner.

Whistleblowing is not an alternative to safeguarding procedures or personal grievance processes. Instead, it operates as a parallel governance mechanism designed to address systemic or organisational issues that may have wider implications for compliance, safety, or ethical conduct.

2. Legal and Regulatory Context

This policy is informed by the Public Interest Disclosure Act 1998 (PIDA), which provides legal protection for individuals who disclose information in the public interest relating to wrongdoing. It is also underpinned by the Employment Rights Act 1996 (as amended), UK GDPR and the Data Protection Act 2018, and where relevant, statutory safeguarding frameworks including Keeping Children Safe in Education (KCSIE 2025/2026 application).

In practice, whistleblowing sits at the intersection of employment law, safeguarding obligations, and organisational governance. This creates a requirement for careful balancing between confidentiality, investigation integrity, and legal compliance. The organisation recognises that effective whistleblowing arrangements are not only a legal requirement but also a critical component of organisational risk management and quality assurance.

3. Definition and Scope of Whistleblowing

Whistleblowing refers to the disclosure of information where an individual reasonably believes that wrongdoing is occurring, has occurred, or is likely to occur, and where such disclosure is made in the public interest.

In a training and education context, this may include concerns relating to financial irregularity, fraud, unsafe practice, failure to meet regulatory requirements, concealment of safeguarding risks, or breaches of legal or professional standards. It may also include concerns about systemic failures in governance or repeated non-compliance with organisational policy.

It is important to distinguish whistleblowing from individual grievances. A grievance typically relates to a personal employment issue, whereas whistleblowing concerns issues that extend beyond the individual and may impact learners, staff, stakeholders, or organisational integrity more broadly.

4. Raising a Concern and Reporting Routes

Concerns should normally be raised internally in the first instance, as this allows the organisation to investigate and respond promptly. However, the policy recognises that there may be circumstances where individuals feel unable to use standard reporting channels.

Where concerns arise, individuals may raise them directly with the Designated Safeguarding Lead, Jennifer Crook, who also holds senior leadership responsibility for organisational governance and safeguarding oversight. She can be contacted via jenny.crook@jctrainingandconsultancy.co.uk or on 07540 285652.

Alternatively, concerns may be raised with the Deputy Designated Safeguarding Lead, Kaley Casson, at kaley@jctrainingandconsultancy.co.uk . A dedicated safeguarding and reporting inbox is also available at safeguarding@jctrainingandconsultancy.co.uk to provide an additional accessible route for disclosure.

The availability of multiple reporting channels is intended to reduce barriers to disclosure and reflect good governance practice, particularly in environments where hierarchical structures may otherwise inhibit escalation.

5. Confidentiality and Anonymity

The organisation is committed to handling all whistleblowing disclosures with a high degree of confidentiality. Information will only be shared with individuals who need to be involved in the investigation or resolution of the concern.

While anonymous disclosures will be accepted and considered, the organisation recognises that anonymity may limit the ability to investigate concerns fully or provide feedback on outcomes. For this reason, individuals are encouraged, where possible, to provide contact details while retaining assurance that their identity will be protected in accordance with legal requirements.

The organisation will not disclose the identity of a whistleblower without consent unless required to do so by law or where there is a significant safeguarding or legal necessity.

6. Protection from Detriment

A fundamental principle of this policy is that individuals who raise concerns in good faith must be protected from any form of victimisation or detriment. This protection is both a legal requirement under PIDA and a critical element of organisational culture.

Detriment may include formal disciplinary action without justification, informal exclusion from professional opportunities, intimidation, bullying, or any behaviour that could reasonably be interpreted as punitive in response to whistleblowing activity.

Any evidence of retaliatory behaviour will be treated as a serious disciplinary matter and may itself constitute gross misconduct. The organisation recognises that without robust protection mechanisms, whistleblowing systems lose credibility and fail to function effectively.

7. Investigation Approach and Governance Oversight

All whistleblowing concerns will be recorded, acknowledged where possible, and assessed for seriousness and urgency. The investigation process will be proportionate to the nature of the concern and may involve senior leadership or an external independent review where appropriate.

Investigations will be conducted objectively, with consideration given to evidential reliability, procedural fairness, and potential conflicts of interest. Where concerns relate to

safeguarding, regulatory compliance, or criminal activity, appropriate external agencies may be engaged.

The organisation recognises that the integrity of the investigation process is central to maintaining trust in the whistleblowing framework. As such, investigations are expected to be timely, well-documented, and free from undue organisational influence.

8. Interface with Safeguarding and Regulatory Reporting

Where whistleblowing concerns overlap with safeguarding issues, they will be immediately escalated into safeguarding procedures and managed under the Designated Safeguarding Lead's authority. This ensures alignment with KCSIE requirements and statutory safeguarding thresholds.

Similarly, where concerns indicate potential breaches of funding rules, regulatory requirements, or criminal conduct, appropriate external reporting mechanisms will be considered. This may include engagement with regulatory bodies or statutory authorities.

This dual-interface approach reflects the reality that whistleblowing issues often sit across multiple governance domains and require coordinated response mechanisms.

9. Record Keeping and Data Protection

All whistleblowing concerns, investigations, and outcomes will be securely recorded in accordance with UK GDPR and organisational data retention policies. Records will be stored securely, access-controlled, and retained only for as long as necessary for legal and operational purposes.

The organisation recognises that whistleblowing records often contain sensitive personal and organisational information. As such, strict access controls and data minimisation principles are applied to ensure compliance and reduce unnecessary exposure.

10. Training and Organisational Awareness

Whistleblowing awareness is embedded within staff induction and ongoing training programmes. Staff are provided with clarity on what constitutes whistleblowing, how it differs from safeguarding and grievance processes, and how to escalate concerns appropriately.

The organisation recognises that effective whistleblowing systems depend not only on policy availability but also on cultural confidence. Staff must feel psychologically safe to raise concerns, which requires consistent reinforcement from leadership and visible commitment to ethical practice.

11. Monitoring, Review and Continuous Improvement

This policy is subject to annual review, or sooner where regulatory changes, organisational restructuring, or serious incidents necessitate amendment. Effectiveness is evaluated through governance oversight, case review learning, and compliance monitoring.

The organisation recognises whistleblowing as a key indicator of organisational health. A functioning whistleblowing system is not evidence of failure but of transparency and maturity in governance practice.

12. Policy Commitment

JC Training & Consultancy Ltd is committed to maintaining a culture where concerns can be raised openly, managed responsibly, and used constructively to improve organisational practice. Whistleblowing is viewed not as a threat to the organisation but as a mechanism for strengthening integrity, safeguarding standards, and ensuring continuous improvement.

WHISTLEBLOWING FLOWCHART

STEP 1: CONCERN IDENTIFIED

An individual identifies suspected wrongdoing, malpractice, or serious organisational risk.

This may relate to:

- Safeguarding failures
- Fraud or financial irregularity
- Unsafe practice
- Regulatory non-compliance
- Ethical misconduct
- Systemic governance failure

STEP 2: INITIAL DECISION – IS THIS WHISTLEBLOWING?

The individual considers:

- Is this a personal grievance? → Use HR grievance route
- Is this a safeguarding concern? → Use safeguarding procedure
- Is this wrongdoing in the public interest? → Whistleblowing route

If uncertain → escalate as whistleblowing and DSL will triage.

JC Training & Consultancy
Publish Date: 31/07/2025
Version 9
Reviewed 11/06/2026
Next review date 01/01/2027
Author: Jennifer Crook – CEO

STEP 3: REPORTING ROUTE SELECTED

Concern can be raised via:

- DSL (Jennifer Crook)
- Deputy DSL (Kaley Casson)
- safeguarding@jctrainingandconsultancy.co.uk

Optional external escalation route if internal reporting is not appropriate.

STEP 4: INITIAL RECORDING & ACKNOWLEDGEMENT

- Concern logged securely
- Time/date recorded
- Nature of issue categorised
- Whistleblower protected under PIDA principles

STEP 5: TRIAGE & RISK CLASSIFICATION

DSL assesses:

- Severity (low/medium/high)
- Safeguarding overlap
- Legal/regulatory implications
- Immediate risk to learners/staff/organisation

STEP 6: INVESTIGATION ROUTE DECISION

Outcome determined:

- Internal investigation
- Safeguarding escalation
- External agency referral (DFE / Police / ICO / HSE)
- Independent review required

STEP 7: INVESTIGATION EXECUTION

- Evidence gathered
- Interviews conducted (if appropriate)
- Documentation reviewed
- Findings analysed

STEP 8: OUTCOME & ACTIONS

Possible outcomes:

- No case to answer
- Policy breach confirmed
- Procedural improvement required
- Disciplinary action
- Regulatory escalation

STEP 9: FEEDBACK & CLOSURE

- Outcome recorded
- Whistleblower informed (where possible)
- Case closed or monitored

STEP 10: GOVERNANCE REVIEW

- Lessons learned logged
- Policy updated if required
- Risk register updated
- Leadership review completed

2. WHISTLEBLOWING INVESTIGATION

CASE HEADER

Case Reference Number:
Date Received:
Received By:
Reporting Route: (Email / Verbal / Anonymous / External)

1. REPORTING PARTY INFORMATION

Name (if provided):
Role (Staff / Learner / Employer / Other):
Contact Details:
Anonymity Requested: (Yes/No)

2. NATURE OF CONCERN

Category:

- Safeguarding-related
- Financial / Fraud
- Governance / Compliance
- Health & Safety
- Ethical misconduct
- Other

Detailed Description of Concern:

3. INITIAL TRIAGE (DSL ONLY)

Risk Level:

- Low
- Medium
- High
- Critical (Immediate escalation required)

Safeguarding Link Identified: Yes / No
Prevent / Criminal Link Identified: Yes / No

4. ACTION DECISION

Action Taken:

- Internal investigation
- Safeguarding referral
- External escalation
- No further action (with justification)

Rationale for Decision:

5. INVESTIGATION DETAILS

Investigation Lead:
Start Date:
Evidence Sources Reviewed:

- Documents
- Emails
- Interviews
- System records
- Financial data

Summary of Findings:

6. OUTCOME

Outcome Category:

- Substantiated
- Partially substantiated
- Not substantiated
- Insufficient evidence

Organisational Impact:

7. CORRECTIVE ACTIONS

Actions required:

- Policy update
- Staff training
- Disciplinary action
- Process redesign

- Regulatory notification

Completion deadlines:

8. CLOSURE

Case Closed Date:
DSL Sign-Off:
Deputy DSL Review (if required):