Counter Fraud and Security Management Policy

Policy Created: February 2026

Last Reviewed:

Next Review: February 2027 (or sooner if significant changes in legislation, guidance, or organisational activities occur)

Reviewed by:

Responsible Officer: CEO

Author: Laurence Clark

Approved by: CEO

Main Contact for Queries: info@pathwaysassociates.co.uk

1. Introduction and Commitment

Pathways Associates CIC is a disabled-led Community Interest Company dedicated to enabling people with learning disabilities, autistic people, and their families to live the lives they choose as equals in their local communities.

We operate with the highest standards of integrity, transparency, and accountability, recognizing that fraud, corruption, or security breaches can undermine our mission and harm the vulnerable people we support. This policy outlines our proactive approach to preventing, detecting, and responding to fraud and security risks, while ensuring our practices are inclusive, accessible, and informed by lived experience.

It aligns with UK best practice for small CICs, including guidance from the Charity Commission, CIC Regulator, NHS Counter Fraud Authority (where relevant to our health/social care partnerships), and data protection laws (UK GDPR/Data Protection Act 2018). This policy supports our Corporate Responsibility Policy, Equality and Diversity Policy, and Safeguarding Policy, embedding counter-fraud and security into our values:

- **Led by lived experience** — Involving disabled people in shaping secure, trustworthy processes
- **Partnership** — Collaborating with stakeholders to build resilience against risks
- **Diversity and respect** — Ensuring measures are accessible and non-discriminatory
- **Innovation** — Using creative, proportionate solutions to protect our community
- **Integrity** — Acting honestly, transparently, and ethically in all dealings

We commit to a zero-tolerance stance on fraud and security breaches, promoting a safe environment where concerns can be raised without fear.

2. Scope

This policy applies to all Pathways Associates CIC activities, including:

- Financial management, procurement, and fundraising
- Data handling (e.g., personal information of disabled people, families, and partners)
- Physical and digital security (e.g., events, remote working, IT systems)
- Partnerships, training, co-production, and internal operations

It covers:

- Colleagues, volunteers, associates, and Experts by Experience
- Partners, suppliers, contractors, and stakeholders
- Any assets, information, or resources under our control

Fraud includes theft, bribery, false representation, or abuse of position. Security covers physical (e.g., event safety), cyber (e.g., data breaches), and information security.

3. Key Objectives

We aim to:

- Prevent fraud and security risks through robust controls and awareness
- Detect issues early via monitoring and reporting mechanisms
- Respond effectively, fairly, and proportionately to incidents
- Protect vulnerable individuals and maintain trust in our disabled-led work
- Learn from incidents to continuously improve, co-producing solutions where appropriate
- Ensure compliance with laws (e.g., Fraud Act 2006, Bribery Act 2010, Computer Misuse Act 1990)

4. Core Principles

Our approach is guided by:

- **Proportionality** — Risk-based measures suitable for a small CIC, focusing on high-impact areas like data and finances
- **Transparency** — Open reporting of incidents (anonymized where needed) and lessons learned
- **Accessibility** — Reporting channels and training designed for diverse needs, including easy-read formats and support for communication
- **Fairness** — Investigations conducted impartially, with natural justice and no discrimination
- **Collaboration** — Working with external experts (e.g., police, CFA) when required
- **Confidentiality** — Protecting whistleblowers and sensitive information

5. Roles and Responsibilities

- **Board of Directors / CEO**
  - Oversee policy implementation and risk assessments
  - Appoint a Counter Fraud Champion (e.g., CEO or nominated lead)
  - Review incidents quarterly and ensure annual reporting in CIC34
- **Counter Fraud Champion / Responsible Officer**
  - Lead prevention efforts, training, and investigations
  - Maintain a fraud/security register and report to the Board
  - Liaise with external authorities if needed
- **All colleagues, volunteers, associates, and Experts by Experience**
  - Comply with policies (e.g., secure data handling, declare conflicts)
  - Report suspicions promptly and confidentially
  - Participate in training and risk awareness
- **Partners and Stakeholders**
  - Adhere to our standards in joint work
  - Report concerns and cooperate in investigations

If fraud involves safeguarding, we follow our Safeguarding Policy and refer to relevant authorities (e.g., police, CQC).

6. Counter Fraud and Security Processes

We embed prevention, detection, and response across our work:

- **Prevention**
  - Conduct annual fraud/security risk assessments (e.g., financial controls, cyber vulnerabilities)
  - Implement controls: Segregated duties, secure IT (e.g., passwords, encryption), supplier due diligence
  - Promote ethical culture through induction and codes of conduct
- **Detection**
  - Monitor transactions, access logs, and feedback for red flags
  - Encourage anonymous reporting via email (info@pathwaysassociates.co.uk) or whistleblowing line
  - Use accessible channels (e.g., verbal reports, advocates)
- **Response and Investigation**
  - Acknowledge reports within 3 working days
  - Investigate promptly and impartially (internal or external if complex), aiming for resolution within 28 working days
  - Take action: Disciplinary, recovery of losses, referrals to police/CFA
  - Offer support to affected parties
- **Learning and Recovery**
  - Review incidents for lessons, updating policies/training
  - Share anonymized learnings co-produced with Experts by Experience

7. Training, Awareness, and Support

We commit to:

- Providing regular training on fraud recognition, security best practices, and reporting (tailored for accessibility, e.g., easy-read materials)
- Raising awareness through team meetings, events, and resources
- Supporting whistleblowers with confidentiality and protection from reprisal

Training draws from best practice (e.g., CFA resources) and is refreshed as needed.

8. Monitoring, Review, and Continuous Improvement

- This policy is reviewed annually or following incidents/legislative changes
- Progress is monitored via the fraud/security register and Board reports
- We welcome feedback to ensure the policy remains effective and inclusive
- Annual summaries are included in our CIC report for transparency

9. Conclusion

Pathways Associates CIC is committed to safeguarding our resources, data, and community through robust counter-fraud and security measures that uphold our integrity and values. By preventing risks, responding decisively, and learning together, we protect our disabled-led mission and ensure trust in our work for better outcomes for all.