Information Governance and Data Protection 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: Liam Vernon (Data Security and Protection Lead)

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 handle personal and sensitive information responsibly to build trust, protect privacy, and support our mission. This policy sets out our framework for information governance (including data quality, security, and management) and data protection, ensuring compliance with UK GDPR, the Data Protection Act 2018, and ICO guidance. It incorporates best practice for small organisations, focusing on proportionality while safeguarding vulnerable individuals.

This policy builds on our existing practices for data security, website privacy, and bring-your-own-device (BYOD) usage, integrating them into a unified approach. It supports our Health and Safety Policy, Corporate Responsibility Policy, and Counter Fraud and Security Management Policy, embedding information governance into our values:

- **Led by lived experience** — Involving disabled people and families in shaping data practices that respect their rights and needs
- **Partnership** — Collaborating with stakeholders, partners, and regulators to ensure secure, ethical data handling
- **Inclusion and respect** — Ensuring data processes are accessible, non-discriminatory, and culturally sensitive
- **Innovation** — Using creative, efficient solutions to manage data risks without creating barriers
- **Integrity** — Acting transparently, accountably, and ethically in all data-related matters

We commit to processing data lawfully, fairly, and transparently, minimising risks, and responding promptly to breaches.

2. Scope

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

- Collection, storage, use, and sharing of personal data (e.g., from Experts by Experience, participants, colleagues)
- Website usage, email marketing, and digital tools
- BYOD and remote working
- Training, events, co-production, and partnerships

It covers:

- All data types: Personal, special category (e.g., health data), and organisational
- Colleagues, associates, volunteers, Experts by Experience, partners, contractors, and service users

Exclusions: This does not cover clinical data if not part of our regulated activities; refer to partners' policies where applicable.

3. Key Objectives

We aim to:

- Ensure data is accurate, secure, and used only for legitimate purposes
- Protect privacy rights and prevent unauthorised access or breaches
- Maintain high data quality to support effective decision-making and services
- Comply with legal requirements, including data subject rights and reporting obligations
- Foster a culture of data awareness and ethical handling
- Learn from incidents to continuously improve governance

4. Core Principles

Our approach is guided by UK GDPR principles:

- **Lawfulness, fairness, and transparency** — Process data with clear consent or legal basis, informing individuals
- **Purpose limitation** — Use data only for specified purposes

- **Data minimisation** — Collect only what is necessary
- **Accuracy** — Keep data up-to-date and correct errors promptly
- **Storage limitation** — Retain data only as long as needed, with secure deletion
- **Integrity and confidentiality** — Protect against unauthorised access or loss
- **Accountability** — Demonstrate compliance through records, assessments, and audits

Additionally:

- Accessibility — Provide information in easy-read or alternative formats
- Proportionality — Tailor measures to our small size and low-risk activities

5. Roles and Responsibilities

- **CEO / Senior Leadership**
  - Overall accountability for compliance and culture
  - Appoint Data Protection Officer (DPO) or lead
  - Oversee data impact assessments and policy reviews
- **Data Protection Officer (DPO) / Lead (Liam Vernon)**
  - Advise on compliance, monitor risks, and handle breaches
  - Act as contact for data subjects and ICO
  - Conduct training and audits
- **All Colleagues, Associates, and Volunteers**
  - Handle data securely and report concerns/breaches
  - Follow BYOD guidelines for personal devices
  - Participate in training and data quality checks
- **Board of Directors**
  - Review governance quarterly, including breaches and risks
  - Ensure resources for compliance

Data breaches must be reported to the DPO immediately.

6. Procedures We implement robust processes for data handling:

- **Data Collection and Processing**
  - Obtain consent or identify legal basis (e.g., legitimate interest for training)
  - Provide privacy notices (as per our website policy) explaining rights and uses
  - Use data classification: Public, internal, confidential, restricted
- **Data Quality and Accuracy**
  - Regularly review and update records
  - Use secure systems for storage (e.g., encrypted databases)
  - Conduct data quality audits annually
- **Security and Access Controls**
  - Implement technical measures: Encryption, firewalls, anti-virus
  - Access on need-to-know basis with role-based permissions
  - BYOD: Devices must have virus protection, passwords; no storage of sensitive data without approval; spot checks by IT lead
- **Breaches and Incidents**
  - Report to DPO within 24 hours
  - Assess and notify ICO within 72 hours if required; inform affected individuals
  - Investigate, mitigate, and log in breach register
- **Data Subject Rights**
  - Respond to requests (e.g., access, rectification, erasure) within one month
  - Provide easy mechanisms via info@pathwaysassociates.co.uk
- **Sharing and Transfers**
  - Use contracts/processors with GDPR compliance
  - No international transfers without safeguards
- **Cyber Security**
  - Follow best practices: Multi-factor authentication, regular updates
  - Train on phishing and secure remote access
- **Website and Marketing**
  - Comply with PECR for emails (opt-in, unsubscribe options via Mailchimp)
  - Manage cookies and tracking as per privacy notice

7. Training, Awareness, and Support

We commit to:

- Annual data protection training for all (accessible formats, covering GDPR, breaches, BYOD)
- Induction for new joiners and refresher sessions
- Resources: ICO guidance, internal handbook
- Support for concerns via DPO or confidential channels

8. Monitoring, Review, and Continuous Improvement

- This policy is reviewed annually or post-breach/legislative changes
- Compliance monitored via audits, DPIAs, and register reviews
- Learning co-produced with Experts by Experience
- Feedback welcomed; annual summaries in CIC report

9. Conclusion

Pathways Associates CIC is dedicated to exemplary information governance and data protection that safeguards privacy while advancing our mission. By handling data with integrity, transparency, and inclusion, we build trust and deliver better outcomes for people with learning disabilities, autistic people, and their families.