Data Security, Protection and Quality Policy

Policy Created: May 2023

Last Reviewed: August 2026

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

Reviewed by: Laurence Clark

Responsible Officer: Liam Vernon (Data Security and Protection Lead)

Approved by: CEO

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

1. Introduction

Pathways Associates CIC is a Community Interest Company that develops and delivers services for people who may be entitled to health and social care support. We work with statutory and non-statutory organisations to ensure individuals can influence the services they receive and take greater control of their lives. To carry out this work, we process a small amount of personal data relating to customers, suppliers and staff. We have a responsibility to ensure that all personal data is treated with respect, kept secure and confidential at all times, and processed in full compliance with data protection legislation.

2. Background

Following the end of the Brexit transition period, UK organisations must comply with two versions of GDPR. The UK GDPR, alongside the Data Protection Act 2018, applies to the processing of personal data belonging to UK residents. The EU GDPR continues to apply when processing the personal data of EU residents. Pathways Associates complies with both where relevant.

3. Definitions

Data protection legislation refers collectively to the UK GDPR, the EU GDPR where applicable, and the Data Protection Act 2018. Personal data is any information relating to an identified or identifiable living person. Anonymised data refers to information that no longer identifies an individual. A data subject is the person to whom the personal data relates. Processing refers to any operation performed on personal data, including storage. A data controller determines the purpose and means of processing personal data. A data processor acts on behalf of the controller. A personal data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. Scope

This policy applies to all staff, including directors, managers, employees, trainees, part-time and fixed-term employees, casual workers, temporary staff and agency workers. It applies to all functions and activities

undertaken by Pathways Associates that involve the use of personal data.

5. Objectives

Our objective is to ensure full compliance with all relevant data protection legislation.

6. Principles

We follow the principles set out in the GDPR. Personal data must be processed lawfully, fairly and transparently. Processing must only take place when a lawful basis applies, such as consent, contract, legal obligation, vital interests or another legitimate purpose. Personal data must be collected for specific, explicit and legitimate purposes and must not be used in ways incompatible with those purposes. It must be adequate, relevant and limited to what is necessary. It must be accurate and kept up to date. It must be retained only for as long as necessary. It must be processed securely at all times.

7. Underpinning Policies and Procedures

This policy is supported by our Business Continuity Plan, which outlines procedures in the event of a security failure or disaster; our IT and Social Media Policy, which provides guidance on the disclosure of personal information; our Staff Guidance on Data Breaches, which explains how to respond to a breach; and our Smart Phone BYOD Policy, which governs the remote processing of data on personal devices.

8. Practices

8.1 Data Protection

We are open and transparent with customers and those acting lawfully on behalf of others. We maintain policies to ensure compliance with UK GDPR and the Data Protection Act 2018. We maintain policies for the controlled and appropriate sharing of information with other agencies, taking account of legislation and consent. Where consent is required, we ensure it is informed, explicit, documented and easy to withdraw. We undertake annual audits to ensure compliance. We acknowledge our accountability for ensuring that personal data is processed lawfully,

collected for legitimate purposes, minimised, accurate, retained appropriately and processed securely. We uphold all personal data rights under GDPR, including the rights to be informed, access, rectification, erasure, restriction, portability, objection and rights relating to automated decision-making.

We have voluntarily appointed a Data Protection Officer (DPO) who reports directly to senior management and is given independence and adequate time to carry out their duties. We complete the Data Security and Protection Toolkit annually. We integrate safeguards into all data processing activities and ensure data protection by design and by default. All new systems incorporate data protection from the outset. All existing processing activities are recorded in our Record of Processing Activities and reviewed annually. We ensure that personal data is only processed when necessary and that the minimum amount of identifiable data is used.

8.2 Data Security Procedures

Physical Access

Staff receive training on safe handling of information during induction. Personal and confidential data must be stored securely in locked storage when not in use. The Information Asset Register records the location of all confidential information. Storage locations are risk-assessed and audited annually.

Digital Access

Access to digital systems is granted on the principle of least privilege. Staff receive training and must sign to confirm understanding of access conditions. Changes to access rights can only be authorised by the Data Security and Protection Lead. Password management procedures are followed. Access rights are revoked immediately when staff leave. Access rights are reviewed at least annually. Screens must be locked when not in use.

Access Monitoring

Compliance checks ensure that administrator rights are restricted, access rights are reviewed, staff log out appropriately, password policies are followed and staff understand how to report breaches.

Data Security Audits

Audits focus on controls within electronic and paper systems. They may include spot checks, electronic reports and reviews of access attempts, previous incidents, staff awareness, consent procedures, access rights, storage arrangements, secure transfer processes, device security, waste disposal and compliance with policies.

Data Security Breaches

Staff must recognise and report potential breaches immediately. A Data Security Breach Incident Report Form must be completed and submitted to the Data Security and Protection Lead. If a personal data breach poses a risk to individuals, the ICO will be notified within seventy-two hours. Individuals affected will be informed without undue delay. Breaches are recorded, investigated and used to improve procedures.

8.3 Data Quality

We ensure data is authentic, reliable, complete, accurate, timely and usable. Service user records document service history and contracts. Staff records document employment details. We use standardised structures, train staff, and ensure individuals can access their records. Staff are responsible for accuracy and completeness.

8.4 Correction of Errors

Individuals have the right to request rectification of inaccurate or incomplete data. We respond within one month, or two months if complex. We may inform third parties where appropriate. Processing is restricted while requests are assessed. Refusals are explained in writing and individuals are informed of their rights.

8.5 Record Keeping

Records follow standardised structures and are stored securely. Records are maintained, updated and shared only with those who have a lawful basis. Individuals may request access, rectification or erasure at any

time. Records are retained only as long as necessary and disposed of securely. Record keeping procedures are audited annually.

8.6 Transparency

Our privacy notice explains why we hold data, our lawful bases and individuals' rights. It is freely available and reviewed annually. Individuals are informed of their rights when contracts are signed. If we receive data from another source, we inform the individual within one month.

8.7 Retention and Disposal

Records are retained according to legislation. At the end of their lifespan, records are appraised to determine whether they should be retained or destroyed. Paper records are securely destroyed. Digital records are deleted from all systems, including backups.

8.8 Information Handling

Personal information is only processed when a lawful basis exists. Staff follow confidentiality guidelines. Personal information is protected during receipt and transfer. Staff take precautions during verbal communication. Postal transfers use signed-for delivery. Portable devices are encrypted, password-protected, security-marked and regularly backed up. Person-identifiable information is only sent via secure email.

8.9 Individual Rights Requests

Individuals may exercise their GDPR rights verbally or in writing. Requests are acknowledged immediately and responded to within one month. Identity verification is required. Requests may be refused if unfounded or excessive. All requests are logged.

8.10 Subject Access Requests

Individuals have the right to access their personal data. We provide copies free of charge unless additional copies are requested, in which case a reasonable fee may be charged. Information is provided in a reasonable format.

8.11 Right to Erasure

Individuals may request erasure in specific circumstances, such as when data is no longer necessary, consent is withdrawn, processing is unlawful or required to comply with legal obligations. We cannot erase data when processing is required for employment assessment, legal obligations, public health, research or legal claims. Third parties may be informed where appropriate. Erasure follows disposal procedures.

8.12 Right to Restrict Processing

Individuals may request restriction while accuracy is verified, when processing is unlawful but erasure is not requested, when data is needed for legal claims or when an objection is being investigated. Restricted data is stored securely and made inaccessible.

8.13 Right to Object

Individuals may object to processing in certain circumstances. They have an absolute right to object to direct marketing, and we will stop immediately. Objections to processing under public task or legitimate interests must include specific reasons. We may refuse if compelling legitimate grounds exist or if processing is required for legal claims.

8.14 Withdrawal of Consent

Individuals may withdraw consent at any time. Withdrawal is as easy as giving consent. Records are updated accordingly. In rare cases, consent cannot be withdrawn if legislation or public interest outweighs the individual's rights.

9. Cyber Security Policy

Cyber security responsibilities sit with the Data Security and Protection Lead. Cyber security involves technologies, processes and systems designed to reduce cyber-attack risks. GDPR requires robust cyber security. We maintain plans to reduce risks such as hacking, cyber fraud and data loss. Cyber security forms part of our risk management strategy and is reviewed by the Board. Staff receive training and guidance. Online training is available through government resources.

All devices must have strong passwords. Passwords must not include personal information or common patterns. Emails, documents and

reports must be password-protected. Passwords must not be shared. Staff may agree to regular password changes.

Encryption safeguards personal data. Mobile phones must use secure authentication. Files should be encrypted. Staff should minimise sharing of personal data online. Public Wi-Fi must not be used for transferring personal data. Home internet must be secure and use up-to-date malware protection. Public Wi-Fi must not be used for online purchases.

Ransomware is a serious threat. Hackers may encrypt systems and demand payment. Public Wi-Fi increases risk. Staff must follow national guidance, ensure backups are checked, antivirus software is running and firewalls are enabled. Suspicious activity must be reported immediately. Incidents must be logged within one hour. Malware increases ransomware risk, so devices must be regularly checked. Reporting must follow national procedures.

Staff must ensure emails are sent securely and to the correct recipient. Suspicious emails or links must not be opened and must be reported.

Cyber-attack reporting must follow strict procedures. Evidence must not be destroyed. Incidents must be logged. Failure to comply may result in significant fines. Stakeholders must be informed. Social media must not be used during incidents. Cyber security breaches form part of our risk management policy.

10. Responsibilities

The Data Security and Protection Lead is responsible for reviewing policies, maintaining records, responding to requests, reporting to senior management, monitoring compliance, ensuring data quality, upholding individual rights, defining policies, completing the DSPT and monitoring information handling. All staff are responsible for the accuracy of data they record and for reporting mistakes. Breaches may result in disciplinary action.

11. Keeping Data Safe and Secure

Pathways follows all procedures necessary to ensure data security. We comply with GDPR and national cyber security guidance. We limit

access to data, limit the number of devices used, train staff regularly and update policies as needed.

12. Compliance

All staff must comply with this policy. Breaches may result in disciplinary action. Failure to comply with GDPR may result in significant fines or enforcement action from the ICO.

13. Governance

This policy is owned by the Data Security and Protection Lead. It forms part of our governance and accountability measures. We maintain transparency through written contracts, policies, logs, risk management procedures, training, malware protection, home-working procedures, accurate reporting and appointment of a DPO. We use a data protection by design approach. Contracts with external organisations include data protection requirements. Records of contracts are retained. Security procedures are monitored. Breaches are reported. The Board receives training and staff receive ongoing training. DPIAs are undertaken where risks exist. Documentation is retained for accountability.

Data protection by design means we consider data protection in all systems and processes, anticipate risks, minimise data use, ensure automatic protection, use plain language, provide transparency, offer privacy controls, use processors with strong guarantees, and use privacy-enhancing technologies. We limit data sharing, inform stakeholders when sharing is required, avoid making data public, adopt a privacy-first approach, limit staff access and limit device use. DPIAs involve consultation, risk assessment, mitigation and ongoing review. The DPO must be involved in all DPIAs. The ICO is consulted only for high-risk plans.

The DPO monitors breaches, ensures compliance, carries out DPIAs, keeps legislation up to date, acts as the ICO contact, maintains records and provides training. Only one DPO may be appointed, but additional specialists may support them. The DPO’s details are published and provided to the ICO. The DPO attends board meetings and is accessible to staff, individuals and the ICO.

14. Approval

This policy is approved by the designated officer and reviewed annually.