Information Governance and Data Protection Policy

Approved by: Board of Trustees

Review Cycle: Every two years

Next Review Due: 2028

Policy Lead: Jackie Rosenberg (Information Governance Lead)

1. Purpose

This policy establishes a single, coherent framework for the lawful, secure, ethical and effective management of all information held or processed by PDT.

The policy applies to all information, regardless of format (paper or electronic), and to all trustees, staff, volunteers, contractors and third parties acting on behalf of PDT.

2. Scope of Information Covered

- Personal data relating to staff, volunteers, clients, service users and other individuals
- Special category (sensitive) data, including health, safeguarding, equality and criminal records information
- Corporate and operational information, including financial records, minutes, emails and reports
- Public information published to promote transparency and accountability

3. Information Governance Framework

Information Governance provides the overarching framework within which policies, standards, roles and procedures ensure that information is obtained fairly and lawfully, recorded accurately and reliably, stored securely and confidentially, used ethically and effectively, shared appropriately and lawfully, and retained only for as long as necessary and securely disposed of.

Information Governance within PDT is organised across the following interlinked themes:

- Information Governance Management
- Data Protection
- Confidentiality
- Records Management
- Information Quality Assurance
- Information Security

4. Data Protection Principles

PDT processes personal data in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025

All personal data must be processed lawfully, fairly and transparently for specified purposes, be adequate, relevant and limited to what is necessary, be accurate and kept up to date, be retained only for as long as required, be processed in line with individuals rights, be protected against unauthorised access, loss or destruction and not be transferred outside the UK without appropriate safeguards.

5. Lawful Basis for Processing

- Performance of a contract
- Compliance with a legal obligation
- Protection of vital interests
- Public interest or official authority
- Consent of the individual
- Legitimate interests, where these are not overridden by individual rights

Where consent is relied upon, it must be freely given, specific, informed and unambiguous, with a clear affirmative action.

6. Rights of Individuals

- Be informed about how their data is used
- Access their personal data
- Request rectification of inaccurate data
- Request erasure where legally applicable
- Restrict or object to processing
- Individuals also have the right to data portability where applicable and rights relating to automated decision-making and profiling.
- Subject Access Requests will normally be responded to within one calendar month of receipt unless legislation permits an extension

Requests to exercise these rights must be made using PDT's Access Request procedures and will be handled within statutory timescales.

7. Information Security and Confidentiality

- Access information only where authorised and for legitimate purposes
- Prevent unauthorised disclosure of information
- Protect information through secure storage, password management and appropriate technical controls
- Avoid storing personal data on personal devices or unapproved local drives
- Protect portable devices and remove data off-site only where essential and secure
- Report all actual or suspected data breaches immediately to the Information Governance Lead

PDT will assess whether notification to the Information Commissioner's Office (ICO) is required.

Where a reportable personal data breach has occurred, the ICO will be notified within 72 hours of PDT becoming aware of the breach where required by law.

Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, PDT will also notify those individuals without undue delay.

Failure to comply may result in disciplinary action and potential legal consequences.

8. Information Sharing and Disclosure

Information is shared only where there is a clear lawful basis, the sharing is proportionate and necessary, and appropriate safeguards are in place.

Personal data may be shared with statutory bodies, commissioners, auditors or partner agencies where required by law or consented to by the individual. Information will be disclosed without consent where legally required.

9. Records Management and Retention

- Accurate and timely record creation
- Secure storage and controlled access
- Regular review of records
- Lawful retention and secure disposal when no longer required

Retention decisions must align with legal, contractual and operational requirements.

10. Openness and Transparency

PDT is committed to openness while protecting confidentiality. Non-confidential information about governance, services, policies and activities will be made publicly available where appropriate, while commercially sensitive and personal information remains protected.

11. Roles and Responsibilities

Roles

Information Governance Lead: Jackie Rosenberg

Responsibilities

- Board of Trustees: Ultimate accountability; approval of policies and oversight of compliance
- CEO / Information Governance Lead: Day-to-day responsibility for IG and data protection compliance, incident management and reporting
- All Staff, Volunteers and Contractors: Personal responsibility for compliance with this policy and associated procedures

  Data Protection Officer: PDT has determined that it is not legally required to appoint a statutory Data Protection Officer. Data protection responsibilities are therefore undertaken by the Information Governance Lead.

12. Training, Monitoring and Review

- Provide Information Governance and data protection training appropriate to roles
- Promote an information-aware culture
- Monitor compliance and investigate incidents
- Review this policy and supporting procedures regularly

13. Related Legislation and Policies

- ICT and Security Policy
- Subject Access Request Procedures

- Disciplinary Policy
- Safeguarding Policies
- Mental Capacity Act (where applicable)

14. Compliance

Compliance with this policy is a condition of employment or engagement with PDT. Breaches may result in disciplinary action and legal consequences for individuals and the organization.

15. Data Protection Impact Assessments (DPIAs)

PDT will complete a Data Protection Impact Assessment (DPIA) where new systems, projects or processing activities where there is a material risk to rights and freedoms and are likely to result in a high risk to the rights and freedoms of individuals.

16. Record of Processing Activities (ROPA)

PDT will maintain records of its processing activities, including categories of personal data processed, purposes of processing, recipients and retention arrangements.

17. Privacy Notices

PDT will provide clear privacy notices explaining how personal information is collected, used, shared, retained and protected.

18. Processor Contracts

Where third parties process personal data on behalf of PDT, written contractual arrangements meeting the requirements of Article 28 UK GDPR shall be in place before processing begins.

19. ICO Registration

PDT maintains registration with the Information Commissioner's Office where required by law and pays the applicable data protection fee.

20. Special Category and Criminal Records Data

PDT processes special category personal data and criminal records information only where a lawful basis and an additional condition under the UK GDPR and Data Protection Act 2018 has been identified.

Processing of criminal records information shall be supported by an Appropriate Policy Document where required by law.

Access to such information shall be limited to authorised personnel with a legitimate business need.

21. Data Protection Complaints

Individuals may raise concerns or complaints regarding PDT's handling of their personal information directly with the Information Governance Lead.

PDT will acknowledge complaints within 30 days and investigate them in accordance with applicable legislation and organisational procedures.