PARTNERS FOR INCLUSION

DATA PROTECTION POLICY

Document Type	Policy PFIPoL71
Action Required	Board Approved
Document Security	External Use
Owner (Dept.)	Human Resources
Date of Issue	February 2024
Date of Review	February 2026
Version	V2.1

Document Control

Document Control History

Version	Revision Date	Revision Description	Next Review Date

CONTENTS

1 Background

Partners for Inclusion provides Policy and Procedures to promote safe and consistent practice across the Organisation. The framework laid down within our policy lets everyone know how we work and reflects our values and mission statement. Our policies and procedures are written to help us as staff of Partners for Inclusion to make good, safe decisions.

None of these documents stand alone, all fit within the larger framework of how we work.

2 Data Protection Policy – What this means to Partners for Inclusion

Partners for Inclusion recognises its statutory duty to comply with all relevant legislation and the duties and obligations resulting from them i.e. General Data Protection Regulation (2016) and the Data Protection Act (2018) – known as GDPR.

3 Purpose

This policy applies to all Trustees, current and former Directors, employees, agency workers, contractors, consultants, people we support, and covers our commitment to meeting our requirements to protect personal data under the Data Protection Act 2018 (also known as UK GDPR) and the General Data Protection Regulation (GDPR).

This policy applies to all members of staff, including casual worker agreement, consultancy agreement or any other contract for services.

4 Definitions

"Personal Data" means any information relating to an identified or identifiable living individual.

5 Principles of Data Protection Act (2018)

Partners for Inclusion will ensure that all personal data that it holds will be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
- adequate, relevant and limited to what is necessary (data minimisation)

- accurate and kept up to date (data accuracy)

- kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation)

- Processed in a manner that ensures appropriate security of the personal data, including protection against accidental or unauthorised access to, or destruction, loss use, modification, or disclosure of personal data (integrity and confidentiality) Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately (please refer to Document Retention Policy available on the website.

Responsibilities

a) Currently our Data Protection Officer is the HR Manager reporting to the CEO with the following responsibilities:

- Keeping up to date with ICO guidance
- In conjunction with L&D reviewing GDPR training
- Advising other staff on GDPR issues
- Handling notifications and subject access requests
- In conjunction with CEO reviewing procedures for security failure or disaster affecting digital systems or mass loss of hardcopy information necessary for the day to day running of Partners for Inclusion
- Annual register with ICO
- Advising CEO of unusual or controversial disclosures of personal data.

b) All Staff

During induction week all staff are required to take part in mandatory data protection training, read, understand, and accept any policies and procedures that relate to the personal data that they handle during the course of their work. These include Data Protection Policy, Employee Handbook, Information Technology Policy.

Existing staff are required to keep up to date on all policies e.g. discussion at team meetings.

Significant breaches of this policy will be handled under Partners for Inclusion disciplinary procedures.

6 Lawful, fair and transparent

To ensure processing of data is lawful, fair and transparent, Partners for Inclusion shall keep and maintain Data Audits to record when and why we process personal data. The data audits shall be kept up to date and fully reviewed on an annual basis.
The Data Audits will record or lawful bases (our reason) for processing any personal data, this must be one of the following as required by legislation:

- consent
- contract
- legal obligation
- vital interests
- public task
- legitimate interest

The way in which we process personal data is detailed within our privacy notices, which are all available on our website www.partnersforinclusion.org . Our privacy notices will be kept up to date and reviewed annually.

Partners for Inclusion is fully committed to meeting the data protection principle of lawfulness, fairness and transparency.

7 Purpose Limitation

Partners for Inclusion will be clear about what our purposes for processing data are from the start. We will record these purposes in our Data Audits and include details in our public privacy notices.
We will not use the personal data for any other purpose unless this is compatible with our original purpose, we get consent, or we have a clear obligation or function set out in law.

8 Data Minimisation

We will make sure that the personal data we are processing is:

- adequate – sufficient to properly fulfil our stated purpose.
- relevant – has a rational link to that purpose; and
- limited to what is necessary – we do not hold more than we need for that purpose.

9 Data Accuracy

Partners for Inclusion will take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact.

We may need to keep the personal data updated, although this will depend on what we are using it for.

If we discover that personal data is incorrect or misleading, we will take reasonable steps to correct or erase it as soon as possible.

10 Storage Limitation

Partners for Inclusion will not keep personal data for no longer than we need it. How long we keep personal data including people we supports' personal information will depend on our purposes for holding the data. We have a separate Document Retention Policy which informs how long we keep personal data for and how it will be erased, anonymised, or removed from our systems.

We may keep personal data for longer for public interest, archiving or historical research, or statistical purposes.

11 Integrity and confidentiality

Partners for Inclusion takes the security of personal data seriously. We do this in a variety of ways including but not limited to:

- data protection and cyber security training for staff.
- technical measures such as passwords, two factor authentication,
- encryptions, clarity on which systems must be used.
- a named Data Protection Officer to provide advice and support.

12 Rights of Individuals

Individuals have the right to access their personal data and any such requests made to Partners for Inclusion shall be dealt with in line with legal requirements, with some limited exceptions.

The General Data Protection Regulation (2016) and Data Protection Act (2018) provides the following rights for individuals in relation to their personal data:

- the right to be informed – we do this by making sure our privacy notices for employees and the people we support are correct and up to date and direct individuals to these notices on our website www.partnersforinclusion.org

- the right to access their own data – any subject access requests must be notified to our Data Protection Officer (DPO) who will co-ordinate a full search of all our systems before responding to the individual within one month, as required by law.

- rectification – we will quickly update any personal data which has been identified as inaccurate or incorrect.

- erasure – we will remove any personal data if an individual request this, unless we have another lawful basis which would prevent this e.g., we cannot delete employee records as we need to keep these to comply with other legislation.

- to restrict processing – where there is a dispute about the accuracy, validity or legality of personal data held by us, an individual has the right to require us to cease processing the data for a reasonable period to allow the dispute to be resolved.

- the right to data portability – we will provide an individual with their data in an accessible format.

- the right to object – complaints or objections to processing personal data will be dealt with quickly and accurately by the nominated Date Protection Officer (DPO).

- rights in relation to automated decision making and profiling – we do not carry out any automated decision making or profiling of any individual.

13 Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All Trustees and staff must be able to identify a suspected personal data breach. A breach could include:

- access by an unauthorised third party to personal data.
- deliberate or accidental action (or inaction).
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data.
- leaving a file on public transport.

Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.

Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the Information Commissioners Office (ICO). The Information Commissioners Office is the independent regulator of information rights. Further information can be found online at https://ico.org.uk/for-organisations/

The breach must be reported within 72 hours of Partners for Inclusion being aware of the breach. The 72 hours begins when we discover the breach not when it happened.

Where there is also a likely high risk to individuals' rights and freedoms, we will inform those individuals without undue delay and report this to the Chair/Deputy Chair with immediate effect.

The DPO will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence. This record will be reviewed annually and reported to the Board,

This policy will be reviewed by the Board, at least every two years unless there are legal changes within the timescale.

Data Protection Policy
Associated policies and procedures

Policy No.	Version no.	Policy name	Approved on
Web site		Employee Privacy Notice	
Web site		People Supported Privacy Notice	
Website		Duty of Candour annual report	April 2024
PFIPol25		ICT and Digital Acceptable Use Policy	May 2024
PFIPol74		Document Retention Policy.	