Pioneering Care Partnership
Data Protection Policy

Aim

PCP takes its responsibilities with regard to the management of the requirements of The Data Protection Act 2018 (UK's implementation of the General Data Protection Regulation - GDPR) very seriously. This policy sets out how PCP manages those responsibilities.

PCP obtains, uses, stores and otherwise processes personal data relating to potential staff and volunteers (applicants), current staff and volunteers, former staff and volunteers, contractors and others with whom it has business, or with whom it communicates, collectively referred to in this policy as data subjects. When processing personal data, PCP is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

1. are clear about how personal data must be processed and PCP's expectations for all those who process personal data on its behalf;
2. comply with the data protection law and with good practice;
3. protect PCP's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights;
4. protect PCP from risks of personal data breaches and other breaches of data protection law.

Scope

This Policy applies to all staff who work for PCP whether full-time, part time or on a casual basis. This Policy also applies to PCP volunteers, including PCP Trustees and work placement students. Failure to comply with this policy may result in disciplinary action.

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on PCP's behalf must read it.

Personal Data Protection Principles

PCP is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below, which require personal data to be:

1. processed lawfully, fairly and in a transparent manner **(Lawfulness, fairness and transparency).**
2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes **(Purpose limitation).**
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed **(Data minimisation).**

5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed **(Storage limitation).**
6. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage **(Security, integrity and confidentiality).**

Rights of Data Subjects

PCP Subjects' **Individual Rights** (unless a data protection law exemption applies). commits to the processing of all personal data in compliance with the Data

Data Subjects have:
1. the right to be **informed** - e.g. Fair processing/privacy notices
2. the right of **access** - e.g. subject access requests (SARs)
3. the right to **rectification** - e.g. have their data corrected
4. the right to **erasure** – e.g. have their data deleted/removed
5. the right to **restrict processing** – e.g. stop their data being used
6. the right to **data portability** – e.g. transfer their data easily
7. the right to **object** – e.g. challenge what we're doing with their data
8. rights in relation to **automated decision making and profiling** – e.g. safeguards to make sure we don't make potentially damaging decisions about them without human involvement.

Responsibilities

Trustees recognise their overall responsibility for ensuring that PCP complies with its legal obligations.

All Employees are responsible for complying with this policy and attending relevant training.

Senior Managers are responsible for ensuring that the policy is reviewed, disseminated and implemented and addressing any concerns raised through this Policy.

Line Managers Managers are responsible for ensuring that all personal data is handled to ensure that good practice is established and followed and that their departments are fully compliant with this policy and supporting procedures.

Volunteers (including work placement students) are responsible for ensuring they follow this policy in relation to Data Protection.

Definitions

Data Controller PCP is the data controller and it determines the purposes for which and the manner in which any personal data are, or are to be processed.

Data Protection Officer The Data Protection Officer is PCP's Head of Business Excellence with responsibility for overseeing data protection and its implementation to ensure compliance with GDPR requirements.

Data Processors (Staff) Any person who processes the data on behalf of PCP the data controller.

Data Subject The identified or identifiable living individual to whom personal data relates.

Related Policies and Procedures

This Policy should be read in conjunction with the following PCP policies:
1. Confidentiality Policy
2. Data Subject Access Procedure
3. Information Sharing Policy and Procedure
4. Personal Data Loss Breach Procedure
5. Employee Data Protection and Privacy Statement

Relevant Legislation

This policy should be read in conjunction with the following legislation:

1. The Data Protection Act 2018 (UK's implementation of the General Data Protection Regulation - GDPR)

Communication

PCP will ensure that:

- All employees are aware of the policy and associated action plans at induction;
- The policy document is available on PCP's intranet;
- Generic training will include examples or reference to this policy;
- This policy is easily accessible by all members of the organisation;
- Employees are informed when a particular activity aligns with this policy;
- Employees are empowered to actively contribute and provide feedback to the policy; and
- Employees are notified of all changes to this policy in a timely manner.

Monitoring and Review

This Policy will be reviewed by Business Excellence annually to ensure that it remains compliant. A full formal review will also take place every 3 years by Senior Management Team as part of the Policy Review Cycle, and approved by the Board of Trustees.

Policy Document Tracking

Action(s)	**Date(s)**
Draft to SMT:	26 November 2019
Approved Policy circulated to SMT:	November 2019
Approved Policy uploaded to shared:	February 2020
Approved Policy circulated to staff:	February 2020
Interim Review Date:	November 2020
Main Review Date:	November 2022
SMT Lead for Review:	Lindsay Sheridan