Pioneering Care Partnership (PCP)

Confidentiality Policy

Aim
PCP must meet its legal and other obligations with respect to confidential information and our employees, volunteers and relevant third parties must know their responsibility to act with due diligence in relation to disclosure and security of personal, confidential or identifiable information. This Policy is a key part of PCP's overall approach to IG (Information Governance) and reflects the provisions of the General Data Protection Regulation (GDPR).

Scope
This Policy applies to all staff who work for PCP whether full-time or part-time, self-employed, employed through an agency or as a contractor. This Policy also applies to PCP volunteers, including PCP Trustees and work placement students.

Definition
Confidentiality is the limitation, where necessary, of the use of information to only authorised persons i.e. the maintenance of privacy. It is not possible to produce a definitive list of all items considered confidential. The following types of information, however, should always be considered as confidential and at no time divulged inappropriately:

Corporate - commercially sensitive information which may jeopardise a development or business opportunity while negotiations are on-going, for example when tendering for contracts for the supply of goods or services.

Employee - all employee data records (both paper-based and electronic), particularly including details of earnings, equality and diversity monitoring, absence records, recruitment processes and any disciplinary or grievance proceedings.

Service Users - data relating to personal and sensitive information of service users, for example names of individuals, postal addresses, email addresses, telephone numbers, national insurance number etc.

Types of Information and Storage
This Policy applies to information in all forms including text, numerical data, images or photographs, sound recordings and videos. Information may be held or stored in many different ways for example on paper or electronically in computers, smartphones, cameras or removable media such as memory sticks and cards, CDs or DVDs etc. It can be exchanged in many ways including by email, SMS (text message), telephone, fax, and in conversation or meetings.

Relevant Legislation
Data Protection Act 2018
In May 2018 the EU General Data Protection Regulation (GDPR) came into force and it has been consolidated into the Data Protection Act 2018. The 6 "principles" of GDPR are that personal data must be:

- Processed lawfully, fairly and transparently

- Collected only for specific legitimate purposes
- Adequate, relevant and limited to what is necessary
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality

Common Law Duty of Confidence
A duty of confidence arises when one person discloses information to another (for example member of staff to employer) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from case law and included in professional codes of conduct. When an individual has died, information relating to that individual remains confidential under the common law.

Other Legislation
All information, held on computer and in manual filing systems is subject to other relevant legislation including The Human Rights Act 1998, The Freedom of Information Act 2000 and Employment Law and these lay down strict conditions about the keeping of information and its disclosure.

PCP will also adhere to the Caldecott Principles, guidelines adopted by the National Health Service (NHS) and other Social Care organisations in order to secure patient and personal information. The Caldecott Principles outline:

- Organisations and individuals should be able to justify the purpose of holding patient information
- Information on patients should only be held if absolutely necessary
- Use only the minimum of information that is required
- Information access should be on a strict need to know basis
- Everyone in the organisation should be aware of their responsibilities
- The organisation should understand and comply with the law

Information about Individuals

It is our Policy that everyone involved with PCP:

- Has the right to expect that information about them will be held in confidence.
- Knows that the information they provide will only be used for the purposes for which it was given.
- Understands that information about them will not be released to any person outside of PCP without their consent unless conditions for breaching confidentiality are met.

Access to Data

Under the General Data Protection Act 2018, individuals have the right to find out what information organisations store about them. These include the right to:

- Be informed about how your data is being used
  Access personal data (Refer to PCP's Data Subject Access Request (DSAR) Policy and Procedure)
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of your data
- Data portability (allowing you to get and reuse your data for different services)
- Object to how your data is processed in certain circumstances

Breaching Confidentiality

A breach of confidentiality is where information is disclosed to someone without the consent of the person or persons who owns that data.

Confidentiality should only be breached in exceptional circumstances such as:

- If we are told something which leads us to believe someone may be at risk of serious harm or abuse, or assisting a serious criminal offence
- If there is a court order for disclosure

The decision on whether to break confidentiality will be decided on a case by case basis and always in conjunction with a Senior Manager.

Reporting and Consequences of Breaching Confidentiality

Actual or suspected breaches in Confidentiality or other incidents including near misses must be reported at the earliest opportunity referring to PCP's Personal Identifiable Information Loss Procedure for guidance. All reported incidents will be logged, investigated and managed in accordance with the relevant procedure. All serious breaches must be reported to the Information Commissioners Office (ICO) within 72 hours.

Responsibilities

All employees (including those employed through an agency or as a contractor) are under legal and contractual obligations to keep personal and other information confidential not only during their employment (or equivalent) but also after it has been terminated. All information including notes and other papers which relate to PCP's activities must be handed in upon termination of employment. No copies can be retained. Any person seeing confidential information not being used, managed or stored in accordance with this Policy is to report it immediately to their line manager and/or the Operations Manager.

Volunteers (including work placement students) are responsible for ensuring they follow this Policy in relation to Confidentiality.

Chief Executive has overall accountability and responsibility for confidentiality and data protection. Operational responsibility is delegated to the Operations Manager.

Human Resources are responsible for ensuring that the Policy is reviewed, disseminated and implemented. Periodically, internal audits will be conducted to ensure confidentiality is being properly maintained across PCP. GDPR training will also be provided to all members of staff and volunteers on a 3 yearly cycle.

Senior Managers are responsible for ensuring requirements of this Policy are met by their teams.

Related Policies and Procedures

This Policy should be read in conjunction with the following PCP policies:

1. Data Protection Policy
2. Information Sharing Policy
3. Data Subject Access Procedure
4. Employee Data Protection and Privacy Statement
5. Personal Data Loss/Breach Procedure
6. Personal Identifiable Information Loss/Breach Procedure

Relevant Legislation

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

1. Data Protection 2018
2. General Data Protection Regulation

Monitoring and Review

This Policy will be reviewed by Operational Management 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 reviewed and approved by PCP Board.

November 2021

Policy document tracking

Action	**Date(s)**
Draft to SMT:	17th November 2021
Approved Policy circulated to SMT:	17th November 2021
Approved Policy uploaded to shared:	17th November 2021
Approved Policy circulated to Board:	13th December 2021
Approved Policy agreed by Board:	13th December 2021
Approved Policy circulated to staff:	13th December 2021
Interim Review Date:	November 2022 (Completed)
Main Review Date:	November 2024
Operational Lead for Review	Vicky Browning
ELT Lead for Review	Nigel Brough