# Pioneering Care Partnership (PCP) Information Governance (IG) Policy

## Aim

This policy is intended to ensure that PCP complies with all relevant information governance legislation and guidance from the National Information Governance Committee and other good practice. The Policy aims to safeguard the organisation against current and potential future threats and also assist the successful implementation of future developments or changes.

## Policy Statement and Principles

Information is a vital asset, both in terms of the support we provide to people (both non-clinical and clinical support) and the management of projects, services and resources. PCP understands that sound Information Governance plays a key part in organisational and clinical governance, planning and performance management. It is of paramount importance that our information is efficiently and effectively managed, in line with legislation. PCP is committed to developing appropriate policies, procedures and management structures to support our information governance approaches ensuring accountability through a robust governance framework.

PCP undertakes to apply information governance effectively and will implement measures to:

- Comply with regulatory and legislative requirements
- Protect information against unauthorised access
- Maintain the confidentiality and integrity of information
- Ensure all breaches of confidentiality and information security, actual or suspected, are reported and investigated, and where necessary consider appropriate remedial action.

## 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.

## Exclusions

This Policy is non-contractual.

## Definitions

**Information Governance** is the set of standards PCP follows to ensure it carries out its duty to maintain full and accurate information and keep that information confidential and secure.

**Information** includes all information, whether electronic or manual (including social media), information systems, networks, applications and all locations (including remote and home working).

**Personal identifiable information** includes, but is not limited to, an individual, name, address, date of birth, NHS number and local identifiable codes or reference numbers, photographs, videos, audio tapes and anything else that may be used to identify a person directly or indirectly. For example, evaluation results or statistical analyses which have very small numbers which may allow individuals to be identified.

**Anonymised Information**, this is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.

**Caldicott Guardian** is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide social services must have a Caldicott Guardian.  PCP would refer to the local authority or NHS Caldicott Guardian where applicable.

**Information Commissioners Office (ICO)** UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

**Data Protection Officer** is the designated person within PCP who is responsible for making sure that the organization follows regulations in relation to collection, storage, use and disposal of personal data.

## Responsibilities

**Trustees** are responsible for ensuring that the organisation is compliant and for approving and reviewing this Policy as part of the review cycle.

**Senior Managers** are responsible for ensuring that the organisation is registered with the Information Commissioners Office (ICO), has a nominated Data Protection Officer and is aware of local Caldicott Guardians.  They are also responsible for developing appropriate policies and procedures to implement effective information governance processes, ensuring that the Policy is reviewed, disseminated and implemented and addressing any concerns raised through this Policy.

**Line Managers** are responsible for ensuring that those they manage or contract are both aware of and understand PCP's information governance policies, procedures and guidance. They are also responsible for ensuring that the procedures and guidance is applied and adhered to in day to day work.

**All Staff, Volunteers, Contractors and Students** are required to process information in accordance with PCP's policies, procedures and guidance in respect of Information Governance and security and adhere to Data Protection Act 1998.

## Related Policies and Procedures

PCP is also committed to the continued development and implementation of a range of measures and procedures to protect and support staff whilst engaging in organisational activities. This Policy should be read in conjunction with the following related policies, procedures or guidance:

- Charter of Service Standards
- PCP Core Values Statement
- Confidentiality Policy
- Data Protection Policy
- Clinical Governance Policy and associated procedures
- Open File Procedure
- Disciplinary Policy and Procedure
- Business Continuity Plans

## Relevant Legislation

Regulations determining PCP's policies and procedures include, but are not limited to, the following standards and legal requirements:

- Data Protection Act 1998.
- General Data Processing Regulations (Due to be enforced May 2018).
- Common Law Duty of Confidentiality.
- Freedom of Information Act 2000.
- NHS Information Governance toolkit (where appropriate)

## Monitoring and Review

This Policy will be reviewed by the Information Governance and ICT Sub Group 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.

**August 2017**

## Policy document tracking

| **Action** | **Date(s)** |
|---|---|
| Draft to SMT: | 27th July 2017, 8th August 2017 |
| Draft to Board: | 21st August 2017 |
| Ratified by Board: | 21st August 2017 |
| Approved Policy circulated to SMT: | 4th September 2017 |
| Approved Policy uploaded to shared: | 4th September 2017 |
| Approved Policy circulated to staff: | 4th September 2017 |
| Interim Review Date: | |
| Main Review Date: | August 2020 |
| SMT Lead for Review | Claire Todd |