MIND IN CROYDON

INFORMATION GOVERNANCE POLICY

1. Introduction

Information is a vital asset, both in terms of the management of individual clients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

2. Purpose of the policy

This Information Governance policy provides an overview of the organisation's approach to information governance; a guide to the procedures in use; and details about the information governance management structures within the organisation.

3. The organisation's approach to Information Governance

Mind in Croydon Ltd undertakes to implement information governance effectively and will ensure the following:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;
- Information governance training will be available to all staff as necessary to their role;
- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

4. Procedures in use in the organisation

This Information Governance policy is underpinned by the following procedures:

- **Records management procedure** that set outs how client records will be created, used, stored and disposed of;
- **Access control procedure** that sets out procedures for the management of access to computer-based information systems;
- **Information handling procedure** that sets out procedures around the transfer of confidential information;
- **Incident management procedure** that sets out the procedures for managing and reporting information incidents;
- **Business continuity plan** that sets out the procedures in the event of a security failure or disaster affecting computer systems;

5. Staff guidance in use in the organisation

Staff compliance with the procedures is supported by the following guidance material:

- **Records management:** guidelines on good record keeping;
- **Staff confidentiality code of conduct:** sets out the required standards to maintain the confidentiality of client information; obligations around the disclosure of information and appropriately obtaining client consent;
- **Access control:** guidelines on the appropriate use of computer systems;
- **Information handling:** guidelines on the secure use of client information;
- **Using mobile computing devices:** guidelines on maintaining confidentiality and security when working with portable or removable computer equipment;
- **Information incidents:** guidelines on identifying and reporting information incidents.

6. Responsibilities and accountabilities

The designated **Information Governance lead** for the organisation is Richard Pacitti.

The key responsibilities of the lead are:

- Developing and implementing information governance procedures and processes for the organisation;
- Raising awareness and providing advice and guidelines about information governance to all staff;
- Ensuring that any training made available is taken up;
- Coordinating the activities of any other staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;
- Ensuring that client data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott Principles (see appendix A);
- Monitoring information handling in the organisation to ensure compliance with law, guidance and local procedures;
- Ensuring clients are appropriately informed about the organisation's information handling activities.

The day to day responsibilities for providing guidance to staff will be undertaken by project managers.

Mind in Croydon Ltd will ensure that sufficient resources are provided to support the effective implementation of information governance in order to ensure compliance with the law, professional codes of conduct and relevant information governance assurance frameworks.

All **staff**, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.

Approval

This policy was approved by the Board of Mind in Croydon Ltd in April 2017.

APPENDIX A Caldicott Principles

The Caldicott Principles revised 2013 are:

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies