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 board has responsibility for ensuring that there is a robust framework in place for maintaining a strong culture of information governance. It does this by:

- Reviewing and approving the Information Governance policy and processes annually;
- Appointing an Information Governance Lead;
- Undertaking Information Governance training as recommended by the Information Governance Lead; and
- Receives reports from the Information Governance Lead on incidents, information governance project plans and progress and overall governance status.

The designated **Information Governance lead** for the organisation is Emma Turner, CEO.

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.
- Reports incidents to the board.

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.

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 confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

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

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

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

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

https://www.gov.uk/government/publications/the-caldicott-principles