Improving Mental Health Provision CIC (IMHP)

DATA PROTECTION POLICY

March 2017

Introduction

1. Improving Mental Health Provision needs to keep certain information about its employees, Directors, volunteers, members, clients and other members of the public to enable it to monitor performance and achievements. It is also necessary to process information so that staff can be recruited and paid, activities organised and legal obligations to funding bodies and government fulfilled.

2. To comply with the law, information must be collected and used fairly,stored safely and not disclosed to any other person unlawfully. To do this, Improving Mental Health Provision must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the Act). In summary these state that personal data must be:

i) obtained and processed fairly and lawfully;

ii) obtained for a specified and lawful purpose and not processed in any manner

incompatible with that purpose;

iii) adequate, relevant and not excessive for that purpose;

iv) accurate and kept up to date;

v) not be kept for longer than is necessary;

vi) processed in accordance with the data subject's rights;

vii) kept safe from unauthorised access, accidental loss or destruction;

viii) not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

3. All IMHP staff and volunteers who process or use any Personal Information must ensure that they follow these principles at all times. In order to ensure that this happens, IMHP has adopted this Data Protection Policy.

1. Any member of staff, Director volunteer, who considers that this policy has not been followed in respect of personal data about him/herself, should raise the matter with the Designated Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed

4. All employees, Directors, volunteers,members,clients and other members of the public have the right to:

- know what information IMHP holds and processes about them and why;
- know how to gain access to it;
- know how to keep it up to date;
- know what IMHP is doing to comply with its obligations under the Act.

The Data Controller and the Designated Data Controllers

5. IMHP as a CIC is under the Data Controller Act, and the organisation is therefore ultimately responsible for implementation.

6. IMHP's Directors are the Designated Data Controllers

Information Held

7. Personal Information is defined as any details relating to a living, identifiable individual. Within IMHP this applies to employees, Directors, volunteers, members, clients and other members of the public such as job applicants and visitors. We need

to ensure that information relating to all these people is treated correctly and with the appropriate degree of confidentiality.

8. IMHP holds Personal Information in respect of its employees, Directors, volunteers, members, clients and other members of the public. The information held may include an individual's name, postal, e-mail and other addresses, telephone and facsimile numbers, subscription details, organisational roles and membership status.

9. Personal Information is kept in order to enable IMHP to understand the history and activities of individuals or organisations within the voluntary and community sector and to effectively deliver services to its members and clients.

10. Some Personal Information is defined as Sensitive Data and needs to be handled with special care (see paragraph 17 below).

Processing of Personal Information

11.All staff and volunteers who process or use any Personal Information are responsible for ensuring that:

• Any Personal Information which they hold is kept securely; and
• Personal Information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

12. Staff and volunteers should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

13. Personal information should be:

• kept in a locked filing cabinet; or
• in a locked drawer; or
• if it is computerised, be password protected; or
• kept on an encrypted USB device which is itself kept securely.

Telephone Conversations and Meetings

14. If personal information is collected by telephone, callers should be advised what that information will be used for and what their rights are according to the Act.

15. Personal or confidential information should preferably not be discussed in public areas of IMHP work premises, within open-plan IMHP office areas, or in public places within ear-shot.. All staff should be aware of the difficulties of ensuring confidentiality in an open plan area and respect the confidential nature of any

information inadvertently overheard. Any notes taken during or after an interview should be of relevance and appropriate. It is recommended that such notes are subsequently filed in a legible and coherent manner and that informal notes are retained for a short period (1 year), in a secure place, before being shredded.

Collecting Information

16. Whenever information is collected about people, they should be informed why the information is being collected, who will be able to access it and to what purposes it will be put. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of IMHP.

Publication and Use of IMHP Information

17. IMHP aims to make as much information public as is legally possible. In particular information about IMHP staff, Directors and members will be used in the following circumstances:

- IMHP may obtain, hold, process, use and disclose information in connection with the administration, management and business activities of IMHP, including making and keeping lists of members and other relevant organisations.

- IMHP may publish information about IMHP and its members including lists of members, by means of newsletters, email, social media or other publications.

- IMHP may confirm to any third party whether or not any person is a member of IMHP.

- IMHP may provide approved organisations with lists of names and contact details of members or other relevant organisations only where the members or other relevant organisations have given their consent.

- IMHP may use information for anything ancillary or incidental to any of the foregoing.

- Names of, and a means of contacting, staff and Directors will be published within publicity leaflets and on the website.

- Photographs of key staff may be displayed at IMHP or placed on the website with their consent.

- IMHP' internal staff contact list will not be a public document and information such as personal mobile telephone numbers or home contact details will not be given out, unless prior agreement has been secured with the staff member in question.

18. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Designated Data Controllers.

Sensitive Information

19. Sensitive information is defined by the Act as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or a third party.

Disposal of Confidential Material

20. Sensitive material should be shredded. Particular care should be taken to delete information from computer hard drives if a machine is to be disposed of or passed on to another member of staff.

Staff Responsibilities

21. All staff are responsible for checking that any information that they provide to IMHP in connection with their employment is accurate and up to date. Staff have the right to access any personal data that is being kept about them either on computer or in manual filing systems.

22. Staff should be aware of and follow this policy, and seek further guidance where necessary.

Duty to Disclose Information

23. There is a legal duty to disclose certain information, namely, information about:
• Child abuse, which will be disclosed to social services; or

• Drug trafficking, money laundering or acts of terrorism or treason, which will be disclosed to the police.

Retention of Data

24. IMHP will keep some forms of information for longer than others. Because of storage problems, information about clients cannot be kept indefinitely, unless there are specific requests to do so. In general information about clients will be kept for a minimum of 7 years after they use the services, unless other bodies, such as funders, require IMHP to keep the information longer.

25. IMHP will also need to retain information about staff. In general, all information will be kept for six years after a member of staff leaves IMHP. Some information however will be kept for much longer, for example, if required by funders. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the Designated Data Controller.

26. A statement about Data Protection will be displayed clearly within public spaces within IMHP's premises and on the website.