MANCHESTER INSTITUTE FOR PSYCHOTHERAPY

DATA PROTECTION POLICY

Introduction

This policy applies to all the personal data and specific categories of data (sensitive, personal data) collected and processed by the Manchester Institute in the conduct of its business, in electronic format in any medium and within structured paper filing systems.

For MIP to comply with the Data Protection Act (GDPR) 2018, information must be; collected and used fairly, stored safely and not disclosed to any other person unlawfully.

This policy applies to all MIP employees, whether permanent, temporary, any contractors, consultants, trainers and students. The Institute and any of its staff or trainers who process or use personal information must ensure they follow the principles at all times by following this Data Protection Policy.

The Manchester Institute is registered with the Information Commissioner's Office (ICO) for collecting and using personal data. The registration reference is: ZA553532. This policy has been written within relevant ICO guidelines.

Objectives:

MIP will ensure that:

* Appropriate procedures are in place for the processing and management of personal data, including technical and administrative security measures to safeguard personal information.

* That staff and trainers are aware of the security procedures they must follow when handling personal and/or sensitive data.

* That there is someone within MIP who has specific responsibilities for data protection compliance.

* A supportive environment and culture of best practice regarding the processing of personal data is provided for staff.

* Staff must understand their responsibilities when processing personal data and that methods of handling that information are clearly understood.

* Staff and trainers will report any actual, near miss or suspected data breach to the Director for investigation and any serious breaches will be reported to the Information Commissioner's office within 72 hours of it being reported.

* Individuals wishing to submit a subject access request and exercise any of other individual rights are fully aware of how to do this and who to contact

* Staff understand that subject access requests (and other relevant requests) need to be dealt with promptly and courteously

* Individuals are assured that their personal data is processed in accordance with the Data Protection principles, that their data is secure at all times and safe from unauthorised access, alteration, use or loss.

* Other organisations/third parties with whom personal data needs to be shared or transferred, meet compliance requirements.

* Any new systems being implemented are assessed using a Data Protection Impact Assessment to determine whether they will hold personal data, whether the system presents any privacy risks, damage or impact to individual's data and that it meets this policy's requirements.

Data Protection Principles and Individual Rights

It is important that everyone using personal data follows the strict rules relating to Data Protection Principles set out in the Act. These specify that personal data must:

* Be processed fairly and lawfully and transparently.

* Be used for specified, explicit and legitimate purposes and shall not be processed in any manner incompatible with that purpose.

* Be adequate, relevant and limited to what is necessary in relation to the purposes.

* Be accurate and, where necessary, kept up to date.

* Not be kept for longer than is necessary.

* Be handled in a way which ensures adequate security of the personal data, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Individual rights as set out in the Act are:

1. The right to be informed how data is being used
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object how data is processed in certain circumstances
8. Rights in relation to automated decision-making and profiling

Breach of the Policy

Any breach of MIP's data protection policy will be taken seriously and may result in more formal action.

Any member of staff or student who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Director in the first instance.

Notification of Data Held and Processed

All staff, students and other users are entitled to:

- Ask what information the Institute holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed of what the Institute is doing to comply with its obligations under the Data Protection Act 2018.

Responsibilities of Staff, Tutors and Students

All staff, tutors and students are responsible for:

- Checking that any personal data that they provide to the Institute is accurate and up to date.
- Informing the Institute of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the Institute may send out from time to time, giving details of information that is being kept and processed.
- Ensure that any details retained by tutors with regard to student course work complies with the policy.
- Ensuring that any personal data which they hold is kept securely.
- Ensuring that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Access to Information

Staff, trainers and students of the Institute have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in filing systems. Any person who wishes to exercise this right should make the request in writing to Director.

Retention of Data

Student data will be retained by the Institute for five years from the completion of their course.

This policy will be reviewed every 18 months and updated a minimum of every 36 months

Reviewed & Revised March 2021