DATA PROTECTION POLICY

To be read in conjunction with:		Confidentiality Policy
Date for review:		October 2018
Priority Policy?		Yes
Seen by staff subgroup		
Agreed by Governance Committee		22nd May 2018
Approved by BOT		
Notes		This policy was taken directly to BOT in May 2018. It is to be reviewed through normal processes to be re-submitted to BOT in **November 2018**
Required Training		Policy forms part of priority policy list covered in staff induction. Policy will be embedded in the organisation through staff workshops.

Head Office:- 22/23 Blayds Yard, Leeds LS1 4AD
www.mesmac.co.uk
Company Number: 2958336 Charity Number: 1040407

Contents

1. Purpose of the policy

1.1 Yorkshire MESMAC is committed to complying with privacy and data protection laws including:

(a) the General Data Protection Regulation (GDPR) and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017.

(b) the Privacy and Electronic Communications Regulation (2003) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003.

(c) all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office (ICO) or any other supervisory authority.

1.2 This policy sets out what we do to protect individuals' personal data.

1.3 Anyone who handles personal data in any way on behalf of Yorkshire MESMAC must ensure that we comply with this policy. **Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions including criminal proceedings.**

1.4 This policy will be amended in line with the policy review schedule and more often where necessary to reflect any changes in legislation, regulatory guidance or internal decisions.

2. About this policy

2.1 The types of personal data that we may handle include details of:

Service Users
Employees
Volunteers
Interns
Placement students
Apprentices
Nurses based at our building
Contractors – to include Counsellors
Trustees

2.2 The Operations Manager (Technical) at Yorkshire MESMAC is responsible for insuring compliance with GDPR and with this policy.

3. Definitions of data protection terms

3.1 The following terms will be used in this policy and are defined below:

3.2 **Data Subjects** include all living individuals about whom we hold personal data, for instance employees or a service user. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal Data** means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as name, address or date of birth) or it can be an opinion (such as a performance appraisal/experience of specific mental health behaviours). It can also include an identifier such as an identification number, location data and an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4 **Data Controllers** are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with legislation.

3.5 **Data Processors** include any person/organisation that processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website hosts, subcontractors or other service providers which handle personal data on our behalf.

3.6 **European Economic Area** includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.7 **ICO** means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

3.8 **Processing** is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to:

(a) collecting

(b) recording
(c) organising
(d) structuring
(e) storing
(f) adapting or altering
(g) retrieving
(h) disclosing by transmission (e.g. by email, post etc.)
(i) disseminating or otherwise making available
(j) alignment or combination
(k) restricting
(l) erasing
(m) destruction

3.9 **Sensitive Personal Data (which is defined as "special categories of personal data" under GDPR)** includes information about a person's:

1) racial or ethnic origin
2) political opinions
3) religious, philosophical or similar beliefs
4) trade union membership
5) physical or mental health or condition
6) gender identity
7) sexual orientation or sexual history
8) genetic data
9) biometric data
10) such other categories of personal data as may be designated as "special categories of personal data" under legislation.

4. Data protection principles

4.1 Anyone processing personal data must comply with six data protection principals set out in the GDPR. We are required to comply with these principals (below) and show that we comply.

4.2 Personal data should be:

a) processed fairly, lawfully and transparently
b) collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes
c) adequate, relevant and limited to what is necessary for the purposes for which it is held
d) accurate and, where necessary, kept up to date

e) not kept longer than necessary
f) processed in a manner that ensures appropriate security of the personal data

5. Processing data fairly and lawfully

5.1 The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

5.2 To comply with this principle, when we receive personal data about a person directly from that individual, which we intend to keep, we need to provide that person with "the fair processing information". In other words we need to tell them:

a) the type of information we will be collecting
b) who will be holding their information, i.e. Yorkshire MESMAC
c) why we are collecting their information and what we intend to do with it
d) the legal basis for collecting their information (for example, we are relying on their consent, or on our legitimate interests or on another legal basis)
e) if we are relying on legitimate interests as a basis for processing data, what those legitimate interests are
f) whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data
g) the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period
h) details of people or organisations with whom we will be sharing their personal data
i) if relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards
j) the existence of any automated decision-making including profiling in relation to that personal data

5.3 Where we obtain personal data about a person from a source other than the person themselves, we must provide that individual with the following information in addition to that listed under 5.2 above:

a) categories of personal data that we hold
b) the source of the personal data and whether this is a public source

5.4 In addition, whether personal data is obtained directly or indirectly, we must also inform individuals of their rights outlined in section 9 below, including the right to lodge a complaint with the ICO and the right to withdraw consent to the processing of their data

5.5 This fair processing of information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing of information is concise, transparent, intelligible and easily accessible.

6. Processing data for the original purpose

6.1 The second data protection principal requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.

6.2 This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as a contact number or email address in order to update a person about our activities it should not then be used for any new purpose, for example to share with other organisations, without first getting the individual's consent.

7. Personal data should be adequate and accurate

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out of date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

8. Not retaining data longer than necessary

8.1 The fifth data protection principle requires that we should not keep personal data longer than we need to for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer

needed. If you think that we are holding out of date or inaccurate data speak to your line manager.

8.2 The YM schedule listing the timelines for retention of different pieces of information reads as follows:

Unsuccessful job application forms	8 weeks
Candidates not appointed at interview but considered as appointable	7 months
Employee records	6 years after end of employment – Any Safeguarding issues to be retained in separate records and for 25 years i.e. Safeguarding to take precedence
Volunteer details	6 years after end of employment
Our/Begin service users	6 years after final use of our services
Counselling clients	Maximum of 7 years
Medical cards	7 years after final use of our services
Accident books	15 years
Safeguarding information	25 years

9. Rights of individuals under the GDPR

9.1 The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of Yorkshire MESMAC must be aware of these rights. They include (but are not limited to):

a) The right to request a copy of any personal data that we hold about them as the data controller, as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored. This is known as subject access rights.
b) The right to be told any available information as to the source of the data where the data is not collected from the person directly.
c) The right to be told of the existence of automated decision making.
d) The right to object to the processing of data where the processing is based on either the condition of public interest or legitimate interests.
e) The right to have all personal data erased unless certain limited conditions apply. This is the right to be forgotten.
f) The right to restrict processing where the individual has objected to the processing.

g) The right to have inaccurate data amended or destroyed.
h) The right to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

10. Data security

10.1 The sixth data protection principle requires that we keep any personal data we hold secure.

10.2 We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.

10.3 When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal information is held on a memory stick or other portable device it should always be encrypted.

10.4 When deciding what level of security is needed your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5 The following security procedures and monitoring processes must be followed in relation to all personal data processed by Yorkshire MESMAC:

(a) Electronic data must not be stored on local drives or removable drives. They must be stored on our secure server where data can be backed up.
(b) Staff must ensure that computer screens do not show confidential information to passers-by and that they log off/lock their computers when left unattended.
(c) Paper documents that hold personal data must be shredded once the document is no longer needed.
(d) Data must always be transferred in a secure manner. (e.g. encrypted/password protected email)
(e) Paper documents that contain personal data must be kept in locked cabinets or drawers.
(f) When traveling or using an outside location staff must keep all data secure.

11. Transferring Data Outside the EEA

11.1 Yorkshire MESMAC does not routinely share data with organisations in other countries. However we cannot be sure of the location of servers, IP addresses or email servers of other organisations we work with.

11.2 The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected.

11.3 The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay. This list may be updated.

11.4 The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring data to organisations in the US.

11.4 No data should be knowingly shared with an organisation outside the EEA without approval from your line manager first.

12. Processing sensitive personal data

12.1 On some occasions we may collect information about individuals that is defined by the GDPR as special categories of personal data and special rules apply to the processing of this data. In this policy we refer to special categories of personal data as “sensitive personal data. (see section 3.9)

12.2 Purely financial information is not technically defined as sensitive personal data by the GDPR. However particular care should be taken when processing such data.

12.3 In most cases, in order to process sensitive personal data we must obtain explicit consent from the individuals involved, making it clear how we are going to use their information.

12.4 There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data without consent. If you are concerned that you are unable to obtain explicit consent speak to the Operations Manager (Technical).

13. Notification

13.1 We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the GDPR, we will consult with the ICO where necessary.

13.2 We will report breaches to the ICO where necessary within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.