



Mental Health Matters Wales Data Protection Policy

Contents	Page
Policy Statement	2
1 Policy scope	3
2 Personal data definitions	3
3 Data protection principles	3
4 Access to personal data	5
5 Data sharing	5
6 Privacy by design	6
7 Roles and responsibilities	6
8 Policy benefits	6
9 Compliance	7
10 Review	7
11 Associated relevant legislation	7
12 Associated Policies	7

Policy Statement

Mental Health Matters Wales (hereafter referred to as MHM Wales) understands the importance of protecting personal information and is committed to complying with the Data Protection Act 2018 which also incorporates the General Data Protection Regulation 2016/679 (GDPR).

MHM Wales is committed to fostering a culture of transparency and accountability by demonstrating compliance with the principles set out in the Act.

The Data Protection Act 2018 (incorporating GDPR) sets out the rules for how organisations must process personal data and sensitive personal data about living individuals. It gives individuals the right to find out what personal data is held about them by organisations and to request to see, correct or erase personal data held.

MHM Wales needs to collect and process personal data about the people (including employees and individuals) it interacts with to carry out its services and projects effectively.

MHM Wales is committed to ensuring employees are appropriately trained and supported to achieve compliance with GDPR.

1 Policy scope

1.11 This policy applies to all personal data and special category personal data collected and processed by MHM Wales in the conduct of its business and applies to both automated personal data and to manual filing systems.

1.12 This policy applies to all MHM Wales's employees, whether permanent, temporary, contractors, consultants or secondees.

2 Personal data definitions

2.1 Personal data is defined in the GDPR:

Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Special categories of personal data relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3 Data protection principles

3.1 The Data Protection Act 2018 (incorporating GDPR) outlines six principles which underpin the handling of personal data. To ensure compliance with the Regulation, MHM Wales must ensure personal data is:

- (a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency).

In practice this means:

- Having a legitimate ground for collecting and using personal data.
- Not using personal data in a way which would have an adverse effect on the individual concerned.
- Being transparent about how you intend to use personal data and provide privacy notices where appropriate.

- Handling personal data in a way the individual would reasonable expect.
 - Ensuring you do nothing unlawful with personal data.
- (b) Collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes (purpose limitation).

In practice this means:

- Being clear about why you are collecting personal data and what you will do with it.
 - Providing privacy notices when collecting personal data.
 - Ensuring any additional processing of personal data is fair.
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

In practice this means:

- Only processing personal data relevant and necessary.
- (d) Accurate and, where necessary, kept up to date (accurate).

In practice this means:

- Taking reasonable steps to ensure the accuracy of any personal data held.
 - Ensuring the source of the personal data is clear.
 - Carefully considering any challenges to the accuracy of personal data.
 - Considering whether it is necessary to update the information.
- (e) Not kept for longer than is necessary for the purpose (storage limitation).

In practice this means:

- Reviewing the length of time you keep personal data for.
 - Considering the purpose you hold the personal data for in deciding whether, and how long, you retain it.
 - Securely deleting information no longer needed.
- (f) Processed in a manner using technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction (integrity and confidentiality).

In practice this means:

- Designing and organising security to fit the nature of the personal data held and the harm which may result from the breach.
- Ensuring the right physical and security measures are in place, backed by robust policies and procedures and reliable, well-trained employees.
- Reporting security breaches promptly so they can be reported to the Information Commissioner's Office within the required 72 hours timescale.

3.2 In addition, the first principle requires one or more grounds for processing must be satisfied for the processing to take place. Many of these relate to the purpose for which you intend to use the data and the nature of the personal information.

3.3 MHM Wales, as the data controller, is responsible for and able to demonstrate compliance with these principles.

4 Access to personal data

4.1 Employees will have access to personal data only where it is required as part of their functional remit.

4.2 All data subjects (including employees and others who interact with MHM Wales) are entitled to make a Subject Access Request to ask MHM Wales whether it holds any personal data relating to them and, if so, to be given a description of and a copy of the personal data. Exemptions may apply in certain circumstances.

4.3 Subject Access Requests are delegated to and co-ordinated by the Human Resource Manager.

5 Data sharing

5.1 Due to being a charity which currently only delivers services in Wales, it is unlikely for personal data to be transferred outside the European Economic Area. However; with the advent of "Cloud Based" services which MHM Wales may utilise to store information in the future, MHM Wales will ensure personal data will not be transferred outside the European Economic Area unless the country or territory can ensure an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

- 5.2 Personal data in any format will not be shared with a third party organisation without a valid business reason, a contract or Data Sharing Agreement in place, or without the data subject's consent.

6 Privacy by design

- 6.1 MHM Wales is committed to meeting the DPA 2018 Act requirement to consider data privacy at the initial design stages of a project as well as throughout the lifecycle of the relevant data processing.
- 6.2 Data Protection Impact Assessments (DPIA) are a key mechanism for meeting this requirement and will be carried out for all new system to ensure privacy risks are considered at an early stage. This allow MHM Wales to demonstrate to data subjects and regulators personal data will be handled in a responsible way and MHM Wales is compliant with the DPA 2018.

7 Roles and responsibilities

- 7.1 MHM Wales's Data Protection Officer (CEO) has overall responsibility for the charities compliance as a data controller and data processor with the Regulation. It is recognised functions relating to data control and data processing is delegated to key members of MHM Wales.
- 7.2 All employees are responsible for ensuring they meet the requirements of the Regulation. They should familiarise themselves with this policy and related documents.

8 Policy benefits

- 8.1 This policy will benefit MHM Wales by:
- Promoting transparency and accountability, and fostering a data protection culture across the charity.
 - Ensuring compliance with the Act.
 - Ensuring employee confidence and compliance in their processing of personal data, being fully informed and aware of their responsibilities and obligations.
 - Reducing the risk of financial penalties (up to £17m) and reputational damage from non-compliance.
 - Providing confidence to those who engage with MHM Wales through demonstrating their personal data is being well managed and ensuring data subjects know how they can access it.

9 Compliance

9.1 Breaches of this policy will be investigated and appropriate actions taken.

10 Review

10.1 This policy will be reviewed annually or as business reasons dictate.

11 Associated relevant legislation

- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- Privacy and Electronic Communications (ED Directive) regulations 2003
- Human Rights Act 2004
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Equalities Act 2010

12 Associated Policies

- GDPR Data Breach Notification Policy
- GDPR Data Protection Policy
- GDPR Policy on Your Rights in Relation to Your Data