Name of Policy & Procedure: Data Protection Status: In place Discussed with Board (Governance & Quality): May 2018 Date: May 2018 Review date: May 2020	mind for better mental health Richmond Borough

DATA PROTECTION POLICY

1 PURPOSE

1.1 The purpose of this document is to protect the rights and privacy of individuals who access Richmond Borough Mind (RB Mind) services, work or volunteer for, or support RB Mind. We will ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge.

1.2 The policy defines the structures and measures in place to protect data about individuals and is intended to ensure that all those who handle personal information are fully aware of their obligations.

1.3 This policy is designed to ensure that RB Mind complies fully with Data Protection Legislation and that personal data will be processed with a lawful basis and in a fair and transparent manner.

2 SCOPE

2.1 "Data Protection Legislation" means the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and, to the extent that it deals with Data Protection, the E-Commerce Directive 2000/31/EC together with any related legislation, regulations or codes of practice.

2.2 The Data Protection Legislation applies to all personal data throughout its lifespan, from the point of collection to its eventual destruction. Personal data includes any piece of information which enables the identification of a living individual, such as a name, contact details and health information. For the purposes of this Policy references to personal data shall include sensitive personal data or special categories of personal data (see 4.6 for definition) unless stated otherwise.

2.3 In most instances it does not matter in what format information is held. If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by the Data Protection Legislation.

2.4 The Policy applies to all staff and volunteers of the organisation and third party contractors. You should familiarise yourself with this Policy and the Confidentiality Policy and comply with their terms when processing personal data on our behalf.

3 PRINCIPLES

3.1 RB Mind holds relevant personal details on service users, carers, employees, donors, trustees and volunteers, as well as information on the financial management of the organisation. This information is held by RB Mind for the purpose of supporting those suffering from mental health issues, and carers, in order for them to access the services they need, and for representing their interests.

3.2 The GDPR lists the following Data Protection principles, to be followed by all organisations. RB Mind affirms its commitment to follow these fully:

- **Lawfulness & Fairness:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- **Purpose Limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data Minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** Personal data shall be accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, is erased or rectified.
- **Storage Limitation:** Personal data shall be kept in a form which allows identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Security:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Sending information outside the EEA:** RB Mind will not send information to an area outside the EEA (European Economic Area) without ensuring the appropriate level of protection for this information.

Overall, this means we must collect and use personal data fairly, tell people how we will use their personal data, store it safely and securely and not disclose it unlawfully to third parties. We need to be careful that the information we collect is relevant and that we do not collect more information than we need for the stated purpose.

3.3 All RB Mind services should display or make available adequate privacy notices to clients explaining how we process their information. We must provide privacy notices even if we do not need to ask for consent.

3.4 Partners and any third parties working with or for the organisation, who may have access to personal data, will be expected to comply with the principles of this Policy. No third party may access personal data held by the organisation without having first entered into an agreement to uphold the terms of this policy.

3.5 RB Mind is registered with the Information Commissioner's Office (the ICO) to process certain information about staff, volunteers, third party contractors, clients and supporters in order to provide the following:

- Provision of Mental Health services
- Fundraising, campaigning and membership services
- Monitoring, evaluation and audit of service provision
- Training

- Employment of staff
- To maintain our own accounts and records.

4 DEFINITIONS

4.1 **Data Asset Register:** A spreadsheet held by RB Mind which details the personal data held, where it is held, the lawful basis for processing it, and how it is processed. The register also contains a list of the Data Processors with whom RB Mind works, and the agreements that we have in place to share data with these organisations.

4.2 **Data Controller:** The organisation (or occasionally, individual) responsible for how and why personal data is used. RB Mind is the Data Controller in its capacity as a collector and manager of information. Any person who handles Personal Data on behalf of RB Mind is bound by the legal requirements of the GDPR, and does not act as an individual but as a representative of the Data Controller.

4.3 **Data Processor:** Data processing is defined as any operation or set of operations which is performed on personal data, whether or not by automated means, (including, but not limited to, collection, recording, organisation, storage, adaptation, disclosure, erasure or destruction). The Data Processor is an organisation (or occasionally, individual) to whom data processing has been outsourced e.g. a payroll provider. For a full list of RB Mind's Data Processors, please see RB Mind's Data Asset Register.

4.4 **Data Subject:** An individual about whom data is held. Data subjects at RB Mind include:

- Mental health service users
- Carers of those with mental health conditions
- Contact details of people in other organisations
- Donors
- Employees and prospective employees including locums and temporary staff
- Trustees
- Volunteers

4.5 **Personal Data:** Data about a living individual who can be identified either from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller.

4.6 **Special Category Data:** Personal data which is particularly sensitive, and needs to be treated with special care, including:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health condition
- Sexuality
- Political opinions
- Criminal record

4.7 **Privacy Notice:** This is a statement by RB Mind explaining what we will do with personal data and why. A copy of our overarching policy is available on our website http://www.rbmind.org/ Service specific information will be provided to individuals at the point of accessing any of our services.

5 INDIVIDUAL'S RIGHTS

5.1 Individuals have the following rights regarding data processing, and the data that is recorded about them:

- **The right to be informed about how we process their personal data** - RB Mind will inform individuals what we do with their data through the appropriate use of privacy notices. More details can be found on our website, and at the point of referral to a service.
- **The right to access their personal data** - RB Mind will respond to subject data access requests in accordance with the regulations (see section 8).
- **The right to rectify their personal data** - If information held about an individual is inaccurate or incomplete, RB Mind will correct it as soon as possible (within one month), after being informed of this. Where it is decided that data will not be rectified, this must be explained to the individual, informing them of their right to complain to the supervisory authority (Information Commissioner's Office (ICO)) and to a judicial remedy. Where there is a disagreement, the individual's views will be recorded on file and attached to the record under question.
- **The right to have their personal data erased** - In health and social care the right to erasure is not absolute, therefore RB Mind will proceed according to appropriate regulation and with the interests of the individual at heart.
- **The right to restrict processing** - RB Mind will restrict processing of personal data when requested by an individual.
- **The right to have a copy of their personal data in a portable form** – Individuals can ask us to provide them or a third party with some of the personal information that we hold about them in a structured, commonly used, electronic form, so it can be easily transferred.
- **The right to object to the processing of their personal data** - RB Mind will respond promptly to all objections to data processing, and, if they are relating to marketing, will stop such processing immediately. If the objection related to other forms of processing, RB Mind will follow ICO guidance, with the interests of the data subject at heart.
- **Rights in relation to automated decision making and profiling** - *This does not apply to the current operations of RB Mind.*

6 DATA COLLECTION

6.1 Data Minimisation is important to think about prior to the collection of any personal data and RB Mind will only collect information that is absolutely necessary.

6.2 As a Data Controller we must ensure that we have a lawful basis for processing all personal data. Under the GDPR there are 6 lawful bases for processing non-sensitive personal data –

- consent
- as is necessary as part of a contract
- to comply with a legal obligation
- to protect the vital interests of an individual
- to fulfil a public task

- as part of the organisation's legitimate interests (provided the latter is balanced against the rights of the individual).

The lawful basis for processing information must be kept up to date in RB Mind's Data Asset Register.

6.3 Stricter rules apply to sensitive personal data (or special categories of personal data), such as information about a person's health, ethnic origin or religious beliefs, as well as information about criminal offences. Due to the nature of our services, we are likely to collect information on an individual's mental health to enable us to provide appropriate support. When such data is collected RB Mind will treat that information with extra care and confidentiality and always in accordance with this policy. The additional justification for processing this information must also be detailed in our Data Asset Register.

6.4 The Data Protection Legislation requires data protection to be taken into account whenever a new system or process is introduced, or where a system or process is changed that involves processing personal data.

6.5 Data Protection Impact Assessments (DPIA) must be completed for any significant changes to how personal data is processed that are likely to result in a high risk to individuals, and where any new technologies or systems are used. For more information please refer to the guidance on https://ico.org.uk/

7 DATA STORAGE

7.1 All staff are responsible for ensuring that any personal data which the organisation holds and for which they are responsible, is kept securely and is not disclosed to any third party; unless that third party has been specifically authorised by the organisation to receive that information and they have entered into a confidentiality agreement. Detailed guidance on this found in the Confidentiality Policy.

7.2 All staff and volunteers must not remove personal data from RB Mind's premises either in electronic or paper form unless it is really necessary – for example, in cases where staff have to attend external meetings. In instances where data is taken out of RB Mind premises, such data must be transported securely (refer to the Confidentiality Policy for appropriate procedure).

8 DATA SUBJECT ACCESS REQUESTS

8.1 Individuals have the right to access their personal data and supplementary information. Where a person requests access to their information, this is called a Data Subject Access Request (DSAR).

8.2 When a subject access request is received, it should be communicated to the Office Manager immediately, so that there is time to comply with the request in a timely manner. RB Mind will provide the information without delay and at latest within 28 days of receipt of the request.

8.3 Data subjects are not entitled to see everything related to their records, as this could compromise the confidentiality of others, so the data needs to be checked and redacted where necessary before it can be supplied to the individual.

8.4 Where requests are complex or numerous, the period of compliance can be extended by a further two months. In this instance, the individual must be informed within one month of the receipt of the request, explaining why the extension is necessary.

8.5 The data must not be changed between receipt of a subject access request and sending the information to the applicant, except for routine amendment of the data which would happen in any case. Unclear terms must be explained as part of the DSAR where relevant.

8.6 A copy of the information must be provided free of charge. Please note that we may, where permitted under applicable law, charge a small administrative fee and/or request proof of identity before accessing records. The fee may apply where the request is manifestly unfounded or excessive, particularly if it is repetitive. The fee may also be applied to further copies of the original material.

9 DATA RETENTION & DISPOSAL OF DATA

9.1 Personal data may not be retained for longer than it is required, e.g. after a member of staff has left the Charity, it may not be necessary to retain all the information held on them. Some data will need to be kept for longer periods than others. Please see Appendix A for more information.

9.2 Personal data must be disposed of securely, in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

9.3 Personal data may need to be kept for a certain period of time under other legislation such as accounting, tax laws, or in the case of legal action. In such cases reasonable measures must be taken to ensure it is kept securely in accordance with industry standards.

9.4 Duplicate copies of personal data should not be kept as doing so increases the risk of that data being compromised.

10 SHARING INFORMATION WITH PARTNER ORGANISATIONS

10.1 Sharing information between partner organisations is vital to the provision of co-ordinated and seamless services where RB Mind's work is delivered in partnership with other organisations. However, any decisions to share information, particularly personal data, must be based on an appropriate risk assessment and the basis for lawful sharing agreed. Templates for forming agreements with Data Processors and other Data Controllers, are available to staff on SharePoint.

10.2 All such relationships will be detailed in RB Mind's Data Asset Register, and RB Mind must inform all individuals at the point of registration if their data is to be shared with a partner organisation.

10.3 When sharing information, in each case, it is important to:

- Identify the lawful basis for sharing the information
- Set out what information will be shared
- Define the common purposes for holding and sharing the information

- Set out how the information will be kept secure

10.4 Personal data will only be shared for a specific lawful purpose or where appropriate consent has been obtained.

10.5 All RB Mind projects delivered in partnership with other third party organisations must include, within the contractual agreement, a clear statement on the extent to which RB Mind and the third party partner organisation is responsible for compliance with Data Protection Legislation (i.e. stating who is the Data Controller and/or Data Processor) and the respective obligations with regard to data protection.

The partner organisations must agree:

- To share personal data with each other where it is lawful and when they are required to do so
- To comply with the requirements of Data Protection Legislation and in particular with the Data Protection Principles
- To inform individuals when and how information is recorded about them and how their information may be used
- To ensure that adequate technical and non-technical security measures are applied to the personal data they hold and transfer
- To promote internal awareness of the protocol
- To have in place procedures to address complaints relating to the disclosure of information.

Each partner to this protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal data whether intentional or unintentional.

10.6 Disclosure of personal data between partners without consent must only be done where it is permitted under the Data Protection Legislation. Details of when this is relevant is detailed in our Privacy Policy and appropriate Privacy Notices.

10.7 RB Mind will review their agreements with any Data Processors and Data Controllers that they are in a contractual relationship with regularly, unless new or revised legislation requires an earlier review.

11 MANAGING A DATA BREACH

11.1 An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused, or has the potential to cause, harm to the rights and freedoms of individuals and/or damage to RB Mind's information assets or reputation.

For example, loss or theft of confidential personal data or equipment, unauthorised disclosure of confidential information, a hacking attack, or human error e.g. sending personal data to the wrong email address.

11.2 Data security breaches include confirmed and suspected incidents, as well as near misses. All suspected information breaches must be reported to your manager and the Office Manager without delay.

11.3 Any breach that is identified by the Office Manager as being potentially serious, or is likely to result in a risk to individuals, must be reported to the CEO without delay.

The CEO then must notify the Information Commissioners Office within 72 hours of RB Mind becoming aware of the breach, and national Mind, if it is considered to be serious.

11.4 If the breach is the responsibility of a partner organisation, RB Mind will assess the potential implications for the individual whose information has been compromised with the organisation responsible for the breach, and agree whether/how to notify the individual(s) concerned; advise the individual(s) of their rights; and provide the individual(s) with appropriate support.

11.5 **Containment and Recovery**
The CEO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to stop the breach and minimise the effect of the breach.

An initial assessment will be made to establish the severity of the breach and the steps required to investigate. This will include establishing whether there is anything that can be done to recover any losses and limit the damage the breach could cause, as well as establishing who may need to be notified as part of the initial containment, including informing the police, where appropriate.

11.6 **Investigation and Risk Assessment**
The CEO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- The type of personal data involved
- The nature, volume and sensitivity of the personal data
- The protections that are in place (e.g. encryption)
- What happened to the data; has it been lost or stolen?
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, the number of individuals involved and the potential effects on those individuals
- Whether there are wider consequences to the breach (e.g. loss of public confidence in a service we provide)

11.7 **Notification**
Based on the type of breach and conclusions of the risk assessment, the CEO will consider whether to notify the ICO and national Mind, the affected individuals, the police, or any other parties – for example, insurers or commissioners/funders.

All data breaches will be reported to RBMind's Board as a matter of course, but where the breach is considered serious, this will be reported immediately to the Chair.

The affected individuals need to be notified without undue delay if the breach is likely to result in a high risk to them. However, this would not be the case if (for example) the information has been encrypted so it is unintelligible to any person who is not authorised to access it.

Notification to the individuals whose personal data has been affected by the incident will include a description of the likely consequences of the breach and the measures taken or proposed to be taken to address the breach. Specific and clear advice will

be given on what they can do to protect themselves, and what action has already been taken to mitigate the risks. Individuals will also be provided with a contact point through which they can contact RB Mind for further information or ask questions on what has occurred.

11.8 An Incident Reporting Form must be completed as part of the reporting process; see the Managing Incidents & Serious Incidents Policy. As part of incident reporting existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

12 IMPLICATIONS OF POOR DATA MANAGEMENT

12.1 Compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage, a detrimental effect on service provision, legislative non-compliance, or fines from the Information Commissioner's Office (ICO). The Charity could be fined if you use or disclose information about other people without their consent or reliance on other lawful grounds.

12.2 Any breach of the Data Protection Legislation or this Policy will be dealt with under the Charity's Disciplinary Policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

13 EQUALITY AND DIVERSITY

13.1 This policy must be applied consistently and in line with RB Mind's Equality and Diversity Policy.

14 MONITORING AND REVIEW

14.1 Overall responsibility for compliance with Data Protection Legislation rests with the CEO. The CEO is responsible for making sure that the data protection function is fully resourced to meet the needs of the Charity and will be responsible for producing procedures for monitoring and review.

14.2 Service Leads are responsible for reviewing data protection awareness and compliance with Data Protection Legislation and this Policy within their teams.

14.3 RB Mind will monitor the policy to ensure consistency, to ensure that it is meeting the needs of the organisation and to make sure that the policy remains compliant with future regulations.

RELEVANT POLICIES

- Communications Policy & Procedure
- Complaints Policy
- Confidentiality Policy
- DBS Information Handling Policy
- Disciplinary Policy
- Email & Internet Policy
- IT Policy
- Finance Procedures

- Managing Incidents & Serious Incidents Policy
- Privacy Policy
- Recruitment of Staff Policy
- Safeguarding Adults at Risk Policy
- Safeguarding Children (Child Protection) Policy
- Social Media Policy
- Volunteer Policy
- Whistleblowing Policy

RELATED DOCUMENTS

- Data Asset Register
- Data Processing Agreement & Terms and Conditions
- Incident Reporting Form
- Personal Information Sharing Agreement – Controller to Controller

Appendix A

DATA RETENTION SCHEDULE

Archiving and deleting data is an important facet to the GDPR 2018, in accordance with the principle that data should not be retained longer than necessary.

In practice, it means that we will need to:

- Review the length of time we keep personal data;
- Consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date.

This annex provides a clear guide to the length of time that data needs to be retained. All data retained needs to be kept in accordance with statutory requirements and this Data Protection Policy[1].

Employee records

Document	Retention Period	Reason for retention period
Personnel files and training records	Six years after employment ceases *(n.b. Senior executives' records should be kept permanently for historical purposes i.e. CEO)*	Limitations Act 1980 & Data Protection Act 1998
Wage/salary records (including overtime and expenses records)	Six years plus the current year	Taxes Management Act 1970
Records relating to working time	Two years from date on which they were made	The Working Time Regulations
Statutory Sick Pay records, calculations, certificates, self-certificates	Three years after the end of the tax year to which they relate	Statutory Sick Pay (General) Regulations 1982
Statutory Parental Leave pay records, calculations, certificates, or other medical evidence	Three years after the end of the tax year in which the parental leave period ends	Statutory Maternity Pay (General) Regulations 1986 The Shared Parental Leave Regulations 2014
Redundancy details (calculations of payments, refunds, notification to the Secretary of State)	Six years after employment has ceased	Data Protection Act
Records relating to events notifiable under the Retirement Benefits Schemes records	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

[1] Data retention periods guided by Buzzacott retention recommendations: http://www.buzzacott.co.uk/getattachment/64ced867-bdc1-4906-862e-6b6fdea1a64e/retention-of-accounting-records-(1

National minimum wage records	Three years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act
Application forms and interview notes (for unsuccessful candidates)	Six months	Disability Discrimination Act 1995 & Race Relations Act 1976
Details re: current pensioners	10 years after benefit ceases	Commercial
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy	Companies Act, Commercial, Pensions Act
Pension contribution records	Permanently	Companies Act, Commercial, Pensions Act

Service user and volunteer records

Document	Retention Period	Reason for retention period
Client records	Three years from last contact	Best practice taken from Care Homes Regulation
Client records (IAPT)	20 years from date discharged or last seen or 8 years after death	Data Protection Act Code of Practice Health and Social Care retention schedules 2016
Client records (Psychotherapy & Counselling)	Seven years from last contact	Best practice
Volunteer Records	Three years from last contact	Best practice
Volunteer applicants who did not start volunteering	Six months from application	Best practice
Incident/Accident records/reports	Three years after the end of investigation	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) & Data Protection Act
Complaint investigations	Six years after the end of investigation	Best practice

Financial records

Document	Retention Period	Reason for retention period
Purchase invoices i.e. petty cash records, invoice (revenue)	Six years from the end of the financial year in which the transaction was made	Companies Act/Charities Act & HMRC
Invoice (capital item)	10 years	Companies Act/Charities Act & HMRC
Successful quotations for capital expenditure	Permanently	Commercial considerations
Income i.e. Bank statements, remittance advices, donations	Six years from the end of the financial year in which the transaction was made	Companies Act/Charities Act & HMRC

correspondence, bank reconciliations, receipts cash book		
Deeds of covenant/Gift Aid Declarations	Six years after the last payment made. 12 years if payments outstanding or dispute regarding the deed	Data Protection Act
Legacies	Six years after the estate has been wound up	Data Protection Act
Transfer pricing documents and other records supporting the company's tax returns	Six years after the end of the accounting period the tax return relates to	Finance Act
Records of all delivery of imports/exports for VAT purposes	Six years from the date the records were created	VAT Act 1994
Payroll tax documentation i.e. P45, tax code notification, annual return	Six years plus current year	Taxes Management Act
Payroll & payroll control account	Six years plus current year	Companies Act/Charities Act & Taxes Management Act

Organisational records

Document	Retention Period	Reason for retention period
Annual Accounts & annual review	Permanently	Data Protection Act, Companies Act, Commercial, Pensions Act
Trustee meeting minutes	10 years from the date of the meeting	Companies Act, Charities Act, Data Protection Act
Contractual agreements with external organisations	Six years after contract end	Limitations Act 1980
Organisational charts	Permanently	Commercial
Employer's Liability insurance certificate	40 years	Employers Liability (Compulsory Insurance) Regulations 1998
Health and Safety records	Three years for general records.	Personal injury actions must generally be commenced within 3 years of injury
Health and Safety records (Hazardous substances)	Permanently	Limitations Act 1980 - unidentified industrial injury actions can be commenced substantially later
Incident/Accident records/reports	Three years after the end of investigation	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) & Data Protection Act

Complaint investigations	Six years after the end of investigation	Best practice
Policies	Three years after lapse	Data Protection Act
Trust deeds and rules	Permanently	Companies Act, Commercial, Pensions Act
Fixed assets register	Permanently	Companies Act, Commercial, Pensions Act
Building deeds	Permanently (or for six years after property is disposed of)	Limitations Act 1980
Leases	12 years after the lease and liabilities under the lease have terminated	Limitations Act 1980
Building planning documents (designs/drawings, planning consent, warranties, health & safety documents)	Permanently (or for six years after property is disposed of)	Limitations Act 1980