



For better
mental health

Richmond Borough Mind

DATA PROTECTION POLICY

1. INTRODUCTION

- 1.1 The Data Protection Act of 1998 came into force in March 2000. It covers any information about an individual from which that individual can be identified. The Act applies to ALL data whether electronic or manual. The Act requires the Richmond Borough Mind (RB Mind) to handle such information responsibly, hold it securely, and release it judiciously. There are eight principles defined in the Act, which govern the handling of information (see Section 3).
- 1.2 RB Mind retains relevant personal details of service users who suffer from mental health distress, carers, and organisations involved with mental health provision and their representatives, fund donors, employees, trustees, volunteers and time bank members. RB Mind also as a charitable body retains information pertaining to the financial management of the organisation that will also be under the jurisdiction of this policy.
- 1.3 The information is held exclusively by RB Mind for the purpose of providing a confidential support and information service to those suffering from mental health distress and their carers in order for them to access the services they need, and for representing their interests.
- 1.4 This document defines the structure and measures in place to protect data about individuals where necessary, in accordance with the Act and follows other guidance set out by RB Mind's Disclosure of Information Policy.

2. DEFINITIONS

- 2.1 '**Data**' includes computerised and manual filing systems that are structured by reference to individuals and readily accessible, for example, card indexes, case file records.
- 2.2 '**Data controller**' is RB Mind in its capacity as a collector of information. Any person who handles Personal Data information on behalf of RB Mind is bound by the legal requirements of the Data Protection Act. Any such person does not act as an individual, but as a representative of the data controller.

- 2.3 **'Data Subject'** is an individual about whom data is held. Data subjects at RB Mind include:
- Mental health service users (be it within RB Mind and / or South West London & St. George Mental Health Trust or any provider)
 - Carers of service users / or those suffering from mental health distress.
 - organisation contact persons
 - donors (individuals or organisations)
 - employees and prospective employees through recruitment
 - trustees
 - volunteers
 - time bank members
- 2.4 **'Personal Data'** means data about a living individual who can be identified from that data.
- 2.5 **'Processing'** means virtually everything from data collection, storage and use to data destruction. There is probably nothing that can be done to personal data that would be outside the scope of this Act.
- 2.6 **'Sensitive Data'** means personal data includes information about:
- racial or ethnic origin of the person;
 - their religious beliefs or other beliefs of a similar nature;
 - their physical or mental health or condition;
 - their sexuality;
 - their HIV status
 - their political opinions;
 - whether they are a member of a trade union;
 - criminal record.
- 2.7 **Finance Data** means any data pertaining to monies generated by the work of the charity through donation or fundraising.

3. THE EIGHT PRINCIPLES OF GOOD PRACTICE

3.1. Personal data shall be processed fairly and lawfully, and if it is sensitive data, with the explicit permission of the data subject. It is fairly and lawfully processed if:

3.1.1 RB Mind is identified as the Data Controller of any information gathered.

3.1.2 Consent is obtained to collect and process personal information (see Section 4).

3.1.3 For sensitive data, explicit consent is obtained where at all possible.

Getting explicit consent may be either impossible or unreasonable where there is confidential counselling, advice or support (see Section 4).

3.1.4 It is also accepted that data of this nature may sometimes be used for monitoring purposes, and in such circumstances safeguards will be in place to ensure that individuals cannot be identified.

3.1.5 The purposes for which the data obtained may be used, as in Principle 2, are explained to the data subject.

3.1.6 Assurance is given that information obtained will not be used for any other purpose than as specified.

3.2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. Information obtained shall be used for the following purposes:

3.2.1 Mailing list, including emailing list

3.2.2 Advice, support and help to individuals be it those in mental health distress or those caring for someone with a mental health difficulty.

3.2.3 Collating statistical data, which may be published, but will in no way cause an individual's personal information to be disclosed except with their consent and following RB Mind Disclosure of Information Policy.

3.2.4 Any other purpose which specifically promotes the aims and objectives of RB Mind, whilst conforming to the requirements of the Act.

Details of the processing of information falling under the Act will be made publicly available on request. This applies whether or not RB Mind is registered under the Act.

3.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

The criterion for collection of information is that it is helpful and useful to the mental health service users and their carers for which RB Mind exists, or that it is relevant to RB Mind's operations. Practical considerations effectively prevent excessive unnecessary data being collected or retained.

Both manual and computer data records allow open-ended insertion of information about an individual, as it is difficult to pre-define precisely the sort of information which needs to be retained. Any open-ended information collected should certainly be relevant to the case in hand.

3.4 Personal data shall be accurate and, where necessary, kept up to date.

Information should always be recorded as accurately as possible and kept up to date whenever new information becomes available. The limited uses to which personal data is put means that out-of-date information should not be prejudicial to a data subject, although it might make the service offered less effective. Where data is processed for statistical purposes, efforts are made to ensure that findings are not biased by factors such as outdated information.

3.5 Personal data shall not be kept longer than is necessary for the purpose(s) under which the data was collected in the first place.

Contacts and donors: kept on file for as long as the relationship with RB Mind lasts.

Employees/Trustees: records are kept for various lengths of time to comply with legal requirements

Volunteers:

Clients: For the entire duration of their contact with services rendered by RB Mind and archived thereafter in accordance with insurers stipulation, data protection and archiving policy.

3.6. Personal data shall be processed in accordance with the rights of data subjects. Personal data is only used for the purposes outlined under Principle 2. Permission to use data for these purposes is requested from the data subject at the time the information is obtained (see also Principle 1). A copy of the information retained on file will be made available to the data subject on request (Section G)

The Act gives rights to individuals in respect of personal data held by others.

The rights are:

- i. Rights of subject access
- ii. Right to prevent processing likely to cause damage or distress
- iii. Right to prevent processing for the purposes of direct marketing
- iv. Rights in relation to automated decision-taking
- v. Right to take action for compensation (see Compensation below) if the individual suffers damage by any contravention of the Act by the data controller
- vi. Right to take action to rectify, block, erase or destroy inaccurate data, and
- vii. Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

Compensation

Under the 1984 Act, data subjects were only allowed to claim compensation through the courts where they had suffered damage as a result of inaccuracy or unauthorised disclosure. This right has been considerably extended to allow the data subject the right to claim compensation for damage caused by any breach of the Act and also for distress in certain circumstances.

3.7 Measures shall be taken to guard against unauthorised or unlawful processing. Personal data, whether held on computer or in physical paper files, should be kept secure at all times (see Section E and section F).

3.8. Personal data shall not be transferred between countries without adequate protection.

The RB Mind computers are connected with computers outside the office utilising many security protocols to protect information transferred. The RB Mind website does not, and will not, contain any information falling under the Data Protection Act. (Incoming information may pertain to an incoming request for RB Mind services or to be added to one of our mailing lists).

4. CONSENT

4.1 It is not strictly necessary to gain the consent of clients before recording information about them, whether the data is Personal Data or Sensitive Personal Data.

4.2 Consent is not necessary for Personal Data where it is your legitimate interests to hold the information, and holding it doesn't harm the data subject.

4.3 There are some circumstances when you need consent to use people's data. For 'sensitive personal data' consent may be required. In other circumstances it is good practice to get consent whenever possible, and this is what the Trust recommends.

4.4 In the case of Sensitive Personal Data there is an exemption from the need for 'explicit consent' in Statutory Instrument (SI) 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000. This exemption covers cases where you are providing a confidential counselling, advice or support service, and getting consent is either impossible or unreasonable (www.hmsso.gov.uk/stat.htm has all the Statutory Instruments).

4.5 Where people are distressed, under pressure, or confused it may make matters worse if you go through a data protection consent procedure, particularly whilst on the phone (see Appendix vii). In these cases it is essential to be aware of the alternative provided by SI 2000 No. 417.

4.6 Consent means at a minimum telling the person what you need the information for and asking whether they mind if you keep it. It is possible that someone may later deny that they gave you this consent. To cover yourself you may wish to obtain a signature using, for example, the Personal Information form, and send it out on initial contact with a new client. However, written consent is not actually a requirement of the Act, but it is good practice to obtain one.

4.7 What constitutes consent? 'Any freely given specific and informed indication of his/her wishes by the data subject signifies their agreement to personal data relating to him being processed'. You cannot infer consent from non-response to a communication. Consent from the 'cared for' and or 'carer's of service users'

4.8 The issue of consent raises the question of data stored on people being cared for or the carers of service users, since RB Mind is not normally in a position to get permission from the cared for or the carers of service users to store this data.

4.9 As described above, there is an exemption from the need for consent in recording sensitive data in the case of confidential support services. So consent from the cared for person or carer of the client is not needed, provided you are only recording information that you need in order to be able to help the carer or the service user.

You should also make sure you mention all potential parties (be it service users or carers of service users) as a data subject category in your Data Protection Notification.

5. STORAGE OF COMPUTER DATA

5.1 Computer security

5.1.1 RB Mind has 10 client computers that are independent and password protected.

5.1.2 Each employee has access to a computer, which can only be accessed by Username and Password. This password is individual to each employee and a list of all passwords are held by the central admin team.

5.1.3 A member of staff supervises log on when a volunteer is going to use computer equipment.

5.1.4 Computers do have access to an external database that is protected via SNL servers. Data-sensitive files on the shared computer drive are protected from unauthorised access by file passwords.

5.2 Memory Sticks

5.2.1 Memory Sticks are used by RB Mind staff to save work related documents when they either work from home or when using any other RB Mind Computer.

5.2.2 Memory Sticks shall not be used to back up work present on any of RB Mind's Computers.

5.2.2 All Staff are to keep work related documents saved on a memory stick to a minimal in order to ensure that if the memory stick is lost no compromise is made related to the above-mentioned act.

5.3 Back Up

5.3.1 All of RB Mind computers may be backed up once a month in order to preserve information produced and to safe guard from any loss of data from any hardware malfunction.

5.3.2 All work related back up will be on an external hard drive that will be stored under lock and key within RB Mind's Central office.

6. STORAGE OF MANUAL DATA

Folder files are kept in a filing cabinet where all information is held. All cabinets are under lock and key with personal contact details and case notes held separately. This information is only accessible to project workers and their managers. Information held on clients is relevant to services they are accessing and any individual case work that is being conducted with them.

7. FINANCIAL DATA

7.1 Financial data is anything to do with the management of the charity's finances and income. This is part of general accounting necessary to safe guard the financial stability of the organisation.

7.2 All data retained will be kept for the period of time specified in annex 1.

7.3 All data will be handled and maintained following RB Mind's financial policy and procedure and the auditing requirements as pre-set by the charity commission.

Annex 1: Archive Policy and Procedure:

1. Introduction

1.1 Archiving Data within an organisation is an importance facet to the data-protection act of 1998. In accordance to the same act and the Freedom of Information Act 2000 information needs to be held for a specific period of time.

1.2 The scope of this annex is to give a clear guide into the length that data needs to be retained. All data retained needs to be kept abiding to the over-arching data protection policy that this annex is apart of.

2. Data Schedule

Record	Statutory Retention Period	Statutory Authority
accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163)
accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985
income tax and NI returns, income tax records and correspondence with the Inland Revenue	not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744)
medical records and details of biological tests under the Control of Lead at Work Regulations 1998	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543)
medical records as specified by the Control of Substances Hazardous to Health Regulations 1999	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 (COSHH) (SI 1999/437)
records relating to children	until the child reaches the age of 21	Limitation Act 1980

records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed.	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894)
wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
actuarial valuation reports	Permanently	None Exist
application forms and interview notes (for unsuccessful candidates)	6 months to a year	None Exist
assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently	None Exist
Inland Revenue approvals	Permanently	None Exist
money purchase details	6 years after transfer or value taken	None Exist
parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance	None Exist

pension scheme investment policies	12 years from the ending of any benefit payable under the policy	None Exist
pensioners' records	12 years after benefit ceases	None Exist
personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases	None Exist
redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	None Exist
senior executives' records (that is, those on a senior management team or their equivalents)	permanently for historical purposes	None Exist
time sheets	2 years after audit	None Exist
trade union agreements	10 years after ceasing to be effective	None Exist
trust deeds and rules	Permanently	None Exist
trustees' minute books	Permanently	None Exist
works council minutes	Permanently	None Exist
Records relating to persons receiving treatment for a mental disorder within the meaning of the Mental Health Act 1983	20 years after the date of last contact between the patient and any health care provider, or 8 years after the patient's death if sooner.	None Exist

3. Storage of Information

RB Mind following the data protection policy will store all of the above-mentioned fields. This encompasses both digital storage via back ups to filling manual data.