Bristol

mind

For better
mental health

Bristol Mind

Data Protection Policy

Bristol Mind

Data Protection Policy

Contents

1. Introduction

This policy was adopted at the Executive of Bristol Mind on 2 April 2003 and replaces any previous policies.

2. General.

Bristol Mind welcomes the 1998 Data Protection Act (hereafter 'The Act') and will endeavour, where possible to have Data Protection procedures that rise above the minimum requirements of The Act.

3. Background.

The 1998 Data Protection Act extends the principle of data protection beyond computer based data (covered by the 1984 Data Protection Act) to include information held within some paper based filing systems, video, audio and photo images. In addition The Act strengthens the Data Protection Principles contained in the 1984 Act and extends the principles to cover all Data Controllers, not just those required to register. The new act also introduces the concept of 'sensitive personal data'.

Bristol Mind will use the Eight Data Protection Principles as guidance for its Data Protection Policy, together with special rules covering 'Sensitive Personal Data'. (see Appendix A).

4. Definitions

For the purpose of this policy:

The *Data Controller* shall be Bristol Mind.

Data Processors shall be those employees, volunteers or trustees, subcontractors, who process data on behalf of Bristol Mind.

Data Subjects shall be anyone whose personal data is processed by Bristol Mind primarily: service users, employees; volunteers; trustees (this list is not exhaustive).

The *Data Protection Compliance Officer* (DPCO) shall be the Coordinator or person appointed by the Trustees.

Personal Data shall be information, concerning living individuals:

Which is stored on any computer (and removable storage media) used by or on behalf of Bristol Mind. This also includes information connected to the work of Bristol Mind held on personal home computers by trustees, staff and volunteers.

Which is stored on any Relevant Filing System used by or on behalf of Bristol Mind. This also includes information connected to the work of Bristol Mind held away from Bristol Mind's administrative office by trustees, staff and volunteers.

A *relevant filing system* is any set of information (not on a computer) which is structured in such a way that information relating to a particular individual is readily accessible.

Data Processing shall be obtaining, recording, transmission, dissemination, altering, collating, blocking, erasing, destroying and use of any personal or sensitive personal data.

The Data Protection Compliance Officer, shall undertake an audit of each area of Bristol Minds activities where data processing takes place, using a pro-forma questionnaire (appendix B) This audit will be used to identify where and how data processing takes place and as the basis of Bristol Mind's entry onto the Data Protection Register. Bristol Mind's entry onto the Data Protection Register shall guide Bristol Minds Data Protection Procedures in Practice.

5. Data Protection Procedures

Wherever possible, Bristol Mind will obtain explicit, written consent to hold and process personal data. Clear information will be given to the data subject as to how and why the data will be processed, how to gain access to any data, correct any entry or prohibit further processing of data.

Where it is not possible to obtain written consent from the data subject, implied consent shall be taken to be:

A request for service provision where the processing of data is necessary for the effective delivery of such a service.

An application for paid or unpaid employment, including trustees, where data processing is necessary to ensure effective personnel recruitment, management and support.

Personal Data will only be obtained and processed for specific purposes, and shall not be further processed in any other manner, without first obtaining the consent of the data subject.

Data shall be accurate, relevant, up to date and not excessive.

Data shall not be kept for longer than is necessary to undertake the purpose for which it was obtained (see appendix C). The purpose and time scale shall be outlined in the relevant section of Bristol Mind's entry onto the Data Protection Register. In some instances the time scale for holding data will be determined by legal requirements.

Holding and processing of data shall be reviewed and revised should there be a significant change in Bristol Mind's relationship with the data subject. eg. Where an employee leaves or a service user ceases to use services.

In accordance with Bristol Mind's open file policy, a data subject will have the right to view any data held on them. Where data is obtained from an identifiable individual belonging to a third party, the individual will be made aware of Bristol Mind's open file policy and offered the opportunity of having any documentation which identifies them (as data subjects) withheld.

Should it be found that information on a data subject is incorrect, inaccurate, misleading or out of date the data subject shall have the right to have the information, corrected, blocked or erased.

6. Access to Personal Data.

Access to personal data shall be restricted to the data subject and to people within Bristol Mind who require access to data in order to carry out their role within Bristol Mind.

Executive Committee members may be given access to personal data not normally available to them should they be investigating any complaint or when dealing with disciplinary/grievance issues. This fact will be relayed to data subjects.

Where a data subject requests access to personal data, Bristol Mind will require sufficient information to confirm the identity of the data subject. Written information will be made available outlining the process for accessing personal data and any fee charged. Bristol Mind will comply with timescales prescribed by law. (40 days at time of writing).

Personal data will only be disclosed to third parties by prior agreement with the data subject or in order to allow the data processor to effectively carry out a given task.

In circumstances where personal data is requested from third parties, Bristol Mind will require sufficient information to confirm the identity of the third party and that appropriate consent has been obtained from the data subject.

Bristol Mind will cooperate in circumstances where the law requires the disclosure of personal data.

7. Protection of Personal Data

Personal Data is confidential and will be protected accordingly. All computer systems will be password protected to prevent unauthorised access to personal data. Password protection will be activated whenever a workstation is left unattended. Infrequently accessed personal data should be stored on removable media and stored in a locked filing cabinet.

Paper based personal data should be kept in locked filing cabinets or locked desk drawers. Personal data should locked away whenever a work station is left unattended.

Access to locked filing cabinets/desks will be restricted to those who need access in order to carry out their role within Bristol Mind.

Personal Data will be disposed of by appropriately eg: shredding for paper-based records, wiping clean or destruction of audio/video tapes.

Data held on computers will be erased using commercially available non-retrieval (‘electronic shredding’) software. Hard drives will be erased using such software prior to disposal of computers.

8. Statements

Application forms, fax messages, emails, publicity material shall carry a brief statement of intent outlining data protection practices (see appendix D).

Appendix. A

The data protection principles

1) Personal data shall be processed fairly and lawfully and, in particular shall not be processed unless –

at least one of the conditions in Schedule 2 is met and
in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2) Personal Data shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

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

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of the data subject under the Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Sensitive Personal Data is:-

Personal data consisting of information as to:

the racial or ethnic origin of the data subject
his/her political opinions

his/her religious beliefs or other beliefs of a similar nature
whether s/he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (consolidation) Act 1992)
his/her physical or mental health or condition
his/her sexual life
the commission or alleged commission by him/her of any offence, or
any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any Court in such proceedings.

NB. Appendix is taken directly from the Data Protection Act which, in line with English law, refers to Data Subjects only in the male gender. The Act applies equally to women.

Appendix B

Retention of Personal Data & Sensitive Personal Data.

Unsuccessful applications for employment or voluntary work, including initial correspondence expressing an interest in a vacancy, will be kept for 6 months after the interview date for a vacancy. After this date, data held electronically will be destroyed. Paper based data will be shredded.

Data held on former employees, will be held for one year after the termination of employment as 'open files', after which, files will be sealed and kept for a further five years. Access to files will only be granted to the data subject and executive committee members (in pursuance of their legal obligations, eg in instances where potential industrial injuries are being investigated).

Data held on service users will be held as 'open files' for three months after the service user ceases to require the support of Bristol Mind, after which files will be sealed and stored securely for a further five years. Access to files will only be granted to the data subject and executive committee members (in pursuance of their legal obligations, e.g. in instances where potential malpractice is being investigated).

Date for which the law or insurers do not prescribe a minimum time for retention will be destroyed within one month of data processing being completed and there being no likely reason for that data to be further processed or stored.

Appendix C – Audit form.

IC	**PRE-AUDIT QUESTIONNAIRE**	**Audit Reference**	
Name of Organisation			
Department/Project			
Address			
Postcode		**Telephone**	
Fax		**E-mail**	
Contact Name			
Position/Job Title			

Work area/or services provided			
Description of sites/ locations to be covered			

DATA PROTECTION QUESTIONS	
Question 1	**Does your project process personal data on individuals?**

Question 2	**What personal information is collected? E.g. name, address, telephone number etc.**
Question 3	**Why do you hold this personal data?**

Question 4	Please provide details of databases/filing systems containing personal data:

IC	**PRE-AUDIT QUESTIONNAIRE**	**Audit Reference**	

DATA PROTECTION QUESTIONS	
Question 5	**Do you hold any sensitive personal information (e.g. medical/health data, ethnic origin etc.)? If so, for what purpose?**

Question 6	How is this sensitive personal information collected?
Question 7	**Who is this sensitive personal information collected from?**

Question 8	Once any personal data has been collected, do you disclose this data to anyone? (If the answer is yes, please provide examples and reasons):

Question 9	**How does your project store personal information? E.g. on computer or manual files or both. What safeguards do you have for storing this information?**		
Question 10	**Who has access to this information?**		
Completed by		**Date**	

Appendix D

Ref No

Bristol Mind
Affiliated Local Association

APPLICATION FORM (Personal Details Sheet)

POST APPLIED FOR: _____

This page will be detached on arrival and will not be seen by the Selection Panel unless you are invited to Interview.

Please complete in black ink or type.

PERSONAL DETAILS
Full Name:
Mr./Ms/Mrs./Miss/other.
Address:

Post Code:
Tel. No. home: work:

REFEREES
Name:
Address:

Tel no.: Relationship to you:
Name:
Address:

Tel no. Relationship to you:

Ref No

Are you related to anyone currently involved with Bristol Mind either paid staff, or a member of the Executive Management Committee?

Have you had any involvement with Bristol Mind in a paid or unpaid capacity? Yes/No

Bristol mind believes that ex-offenders, like every other applicant, should be considered for paid/voluntary work on the basis of their commitment and ability to do the job. However, paid and volunteer staff will be required to work with groups of people deemed vulnerable by the Rehabilitation of Offenders Act 1974.

Do you have any criminal convictions, which you feel we need to know about? YES / NO
Please declare any criminal convictions, which relate to the handling of finance, fraud, or thefts or crimes against persons.

If called for interview, are there any access issues or other factors, which would ensure it is comfortable and accessible to you? Yes/No

All the information I have given here is true. I consent to the use of all this information for considering my application, and understand that:

It will be treated confidentially at all times in accordance with the 1998 Data Protection Act
If I am successful it will form part of my personnel records
If I am unsuccessful the information will be destroyed after six months
Signed **Date**