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 North Staffs Mind (NS 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 NS 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, and volunteers. NS 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 NS Mind for the purpose of providing a confidential support and information service to those suffering from mental health distress and their carers/parents 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 NS 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 NS Mind in its capacity as a collector of information. Any person who handles Personal Data information on behalf of NS 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 NS Mind include:

- Mental health service users
- Carers/parents of service users / or those suffering from mental health distress.
- organisation contact persons
- donors (individuals or organisations)
- employees and prospective employees through recruitment processes.
- trustees
- volunteers.

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 which 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

The eight principles around processing personal data are listed below with further explanation on how these principles apply to NS Mind.

Data must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes
3. Adequate, relevant and not excessive;
4. Accurate;
5. Not kept longer than necessary;
6. Processed in accordance with the data subject's rights;
7. Secure;
8. Not transferred to countries without adequate protection.

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 NS 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 with a mental health issue or those caring for someone with a mental health issue.

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 NS Mind Disclosure of Information Policy.

3.2.4 Any other purpose which specifically promotes the aims and objectives of NS 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.

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, or that it is relevant to NS Mind's service delivery. 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 updated whenever new information becomes available. The limited uses to which personal data are put mean 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.

3.6 Personal data shall be obtained only for one or more specified and lawful purpose.

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

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

Service Users: For the entire duration of their contact with services delivered by NS 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.

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

1. Rights of subject access
2. Right to prevent processing likely to cause damage or distress
3. Right to prevent processing for the purposes of direct marketing
4. Rights in relation to automated decision-taking
5. Right to take action for compensation (see Compensation section below) if the individual suffers damage by any contravention of the Act by the data controller
6. Right to take action, to rectify, block, erase or destroy inaccurate data, and
7. 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.

Access to Data

NS Mind will appoint a Data Protection Compliance Officer.

A request for access to any personal data that relates to an employee or service user should be made by written request using NS Mind's Data Access Request from which can be obtained from NS Mind's head office. A fee of £10 or such a higher amount as permitted by law is payable before access is granted. The completed form must be returned to the Data Protection Compliance Officer with the required fee.

On receipt of request it is our policy to provide copies of all data that we are obliged to disclose within 40 days of receipt of the request by the Data Protection

Compliance Officer.

If a period of less than one year has elapsed since any previous request for access to data was complied with it is unreasonable to expect us to be obliged to comply with a further request before a year has elapsed, unless there are exceptional circumstances.

Should an individual wish to bring any inaccuracy in disclosed data to our attention they must do so in writing. In appropriate circumstances it may be of benefit to arrange an appointment to hand in a written notification of any inaccurate data.

It is NS Mind's policy to ensure that all data is as accurate as possible and all necessary steps to ensure that this is the case and to rectify any inaccuracies will be taken.

Where we have requested a reference in confidence from a referee and that reference has been given on terms that it is confidential and the person providing it wishes that it should not be disclosed to the individual concerned it is the policy of NS Mind that it would be unreasonable to disclose the contents of such a reference unless the consent of the person who gave the reference can be obtained.

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.

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

NS Mind's computers are connected with computers outside the office utilising many security protocols to protect information transferred. The NS Mind website does not, and will not, contain any information falling under the Data Protection Act. (Incoming information may pertain to incoming request for NS 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 in our legitimate interests to hold the information, and holding it doesn't harm the data subject.

4.3 There are some circumstances when we 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 recommended.

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 we are providing a confidential counselling, advice or support service, and getting consent is either impossible or unreasonable (http://www.hmso.gov.uk/stat.htmhas all the Statutory Instruments).

4.5 Where people are distressed, under pressure, or confused it may make matters worse if we go through a data protection consent procedure, particularly whilst on the phone.

4.6 Consent means at a minimum telling the person what we need the information for and asking whether they mind if we keep it. It is possible that someone may later deny that they gave us this consent. To cover ourselves we may wish to obtain a signature using, for example, the project specific referral/application 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/her being processed'. You cannot infer consent from non-response to a communication.

4.8 Consent from the 'cared for' and/or 'carers of service users'. The issue of consent raises the question of data stored on people being cared for or the carers of service users, since NS 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 we are only recording information that we need in order to be able to help the carer or the service user.

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

4.10 There may be situations where NS Mind works in partnership with other organisations on specific projects which require data sharing. NS Mind will clarify which organization is to be the data controller and will ensure that the data controller

deals correctly with any data which is collected.

4.11 Employees can be criminally liable if they disclose knowingly or recklessly personal information outside of NS Mind's policies and procedures.

5. STORAGE OF COMPUTER DATA

5.1 Computer security

5.1.1 NS Mind has computers that are both independent or networked and password protected.

5.1.2 Each employee has access to a computer, which can only be accessed by a Username and Password.

5.2 Memory Sticks

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

5.2.2 Memory Sticks shall not be used to back up confidential work present on any of NS Mind's computers.

5.2.2 All staff who keep work related documents saved on a memory stick must be kept to a minimum 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 NS Mind's paid staff members are allocated a personal storage area on the NAS (Network Attached Storage) at all offices which is only accessible from NSM hardware. Key members of Staff such as Management team and finance records have there own secure space which is only accessible to that individual and the I.T Co-ordinator. This storage space is automatically backed up when any changes have been made, in order to preserve information produced and to safeguard from any loss of data from any hardware malfunction. Both Marsh Street and King Street offices have NAS Drives, which back up to each other daily to provide a secure offsite backup. Other NS Mind offices will have backup systems in place, dependent on specific requirements of that office and any client data (if any) that is stored at that particular site.

5.4 Communal digital file resources – Dropbox

NSM computers have Dropbox software installed, the I.T Co-ordinator holds the 'master' account where all communal digital resources are retained. This includes items such as standard paperwork, policies and procedures, useful information etc. This service is only permitted to provide staff access to general documents between the various NSM offices. The Dropbox is not used for the storage of confidential data.

5.5 Future Developments – Cloudbased Client Management System

NSM will be implementing a Cloudbased Client Management System during 2015/16 all necessary checks and certification will be carried out on the supplier of the system to ensure that it complies with DPA regulations on data storage and how such data is exchanged with NSM systems.

6. STORAGE OF MANUAL DATA

Folder files are kept in filing cabinets where all information is held. All cabinets are under lock and key and keys are then also locked in a key safe. This information is only accessible to counsellors, volunteer and placement counsellors, and project workers and their managers. Information held on service users is relevant to services they are accessing and any individual case work that is being conducted with them.

Files pertaining to employees' personal information are stored in locked cabinets within the Finance Officer and Chief Executive's offices.

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 the general accounting necessary to safeguard the financial stability of the organisation.

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

7.3 All data will be handled and maintained following NS Mind's financial policy and procedures and auditing requirements.

Appendix 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 Appendix is to give a clear guide into the length that data needs to be retained. All data retained needs to be kept in line with the over-arching Data Protection Policy that this appendix is a part 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 (COSHH) 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 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)
Records relating to the recruitment of employees	6 Months to 1 Year	None Exist

Criminal Records Bureau (CRB) disclosure documents	Disclosure form retained for 6 months only	None Exist
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
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/tapes	Permanently	None Exist

3. Storage of Information

NS Mind, in accordance with this Data Protection Policy, will store all of the above-mentioned fields. This encompasses both digital storage via back-ups to filing manual data.

Specific details on how documents/information relating to service users are destroyed or retained is detailed in NS Mind's Confidentiality Policy.

Date of Draft	**August 2011**
Date of Implementation	**Sept 2011**

Date of next review	**August 2016**