Data Protection Policy

1. Introduction and background

1.1. About this policy

This policy sets out how North Staffs Mind seeks to protect personal data of our staff, volunteers, clients and supporters. It sets out the policy framework for staff to understand the rules governing their use of personal data to which they have access to in the course of their work to ensure that personal data is not used, stored or disclosed without such individual's knowledge and is processed with a lawful basis and in a fair and transparent manner.

1.2 Policy Statement

North Staffs 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 including counselling and housing
- Fundraising and campaigning activity
- Monitoring, evaluation and audit of service provision
- Training delivery.

1.3 GDPR

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which strengthens and unifies data protection for individuals within the EU, replacing the Data Protection Act (DPA). After Brexit EU GDPR has been adapted to UK (GDPR) for the UK.

New elements and enhancements aim to create greater consistency between organisations, clear consent, ensure data protection by design, invoke strong penalties, mandatory breach reporting and enhancements on the protection and use of the subject's data, for example, the right to be forgotten.

1.4 Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes for North Staffs Mind includes the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice. • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.

	• Ensuring business policies are adhered to (such as policies covering email and internet use). • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information • Investigating complaints. • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments. • Monitoring staff conduct and disciplinary matters. • Marketing our business. • Improving services.
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency/contract and other staff, clients, suppliers, volunteers, fundraisers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and bank details, details of qualifications and certificates, education and skills, marital status, nationality, CVs and client related information such as NHS numbers, GP contact etc.*
Sensitive personal data	Personal data about an individual's racial or ethnic origin, religious or similar beliefs, physical or mental health or condition, gender, sexuality, criminal offences or related proceedings – any use of sensitive data should be strictly controlled in accordance with this policy.

2 Data Processing at North Staffs Mind

2.1 Who is in charge of data?

We are a "data controller" for the purposes of the Data Protection Act 2018 and the UK General Data Protection Regulation. This means that we are responsible for the processing of your personal information.

We have considered whether we are required to formally designate a Data Protection Officer who is external to North Staffs Mind and have concluded that we do not carry out processing on a significant enough scale to warrant this.

The Chief Executive holds responsibility for ensuring that North Staffs Mind complies with its Data Protection responsibilities. The Chief Executive will ensure that the Council of Management is kept apprised of data protection responsibilities, risks and issues.

Data protection policy and procedures will be reviewed on an annual basis.

2.2 Processing data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (eg. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to who it will be disclosed.

2.3 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Chief Executive.

2.4 Your personal data

You must take reasonable steps to ensure that the data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform your counsellor or our administration team so that we can update your records.

2.5 Data security

You must keep personal data secure against loss of misuse. Where other organisations process personal data on our behalf the Chief Executive will establish what, if any, additional specific data security arrangements need to be implemented in agreements with external partners.

2.6 Storing data securely

- In cases when data is stored on printed paper it should be kept in a secure place where unauthorised personnel cannot access it (ie locked cupboards or filing cabinets).
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The Chief Executive must approve any cloud used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with North Staffs mind's backup procedures.

- Data should never be saved directly to mobile devices such as laptops, tablets or smart phones.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

2.7 Data retention

We must retain data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained for, but should be determined in a manner consistent with our data retention guidelines. (See Appendix 1).

All client records and notes are the property of North Staffs Mind and are held in a secure manner for 6 years following the end of therapy. Records of vulnerable adults or children where risk or safeguarding concerns have been identified will be kept for a longer period to satisfy contractual obligations. Practitioners are not allowed to keep their own notes outside of North Staffs Mind. This policy does not contravene the right of a client to request access to their records, in line with GDPR. Requests for access must be forwarded to the North Staffs Mind's Data Protection Officer for handling.

2.8 Transferring data internationally

There are restrictions on international transfers of personal data outside the UK and information should not be transferred outside of the UK unless it meets the requirements of the Data Protection legislation. Any such transfers require approval from the Chief Executive.

3 Subject Access Requests

Under GDPR individuals are entitled, subject to certain exceptions, to request access to the information held about them. If a member of staff receives a subject access request, they should refer that request immediately to datacontrol@nsmindorg.uk

3.1 Processing data in accordance with individual rights

We will abide by requests from individuals not to use personal data for direct marketing purposes. The Chief Executive will be notified about any such request.

We will not send direct marketing material to anybody electronically unless we have an existing business relationship with them in relation to the services being marketed.

4 GDPR provisions

4.1 Privacy Notice

Being transparent and providing accessible information to individuals about how we will use their personal data is important to our organisation. Our Privacy Statement is available on our website at https://nsmind.org.uk/privacy/. Service users will be given a GDPR Consent Notice which sets out how we use their personal information (See Appendix 3).

4.2 Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy statement (see 4.1 above).

4.3 Justification for personal data

We will process personal data in compliance with all six data protection principles:

- Lawfulness and fairness
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security).

We will document the additional justification for the processing of sensitive data and will ensure that any information of this nature will be treated with extra care and confidentiality and always in accordance with our Privacy Statement.

4.4 Data portability

Upon request a data subject should have the right to receive a copy of their data in a structured format. These Subject Access requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. We can refuse or charge for request that are manifestly unfounded or excessive.

4.5 Right to be forgotten

A data subject may request that any information held on them is deleted or removed. An erasure request can only be refused if an exemption applies.

4.6 Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Chief Executive will be responsible for conducting Privacy impact Assessments and ensuring that all new services commence with a privacy plan.

4.7 Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

4.8 Reporting breaches

The Information Commissioner's Office (ICO) requires certain types of data breaches (where it is likely to result in a risk to the rights and freedoms of individuals) to be reported within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures, thus allowing us to:

- Investigate the failure and take remedial steps where necessary;
- Maintain a register of compliance failures;
- Notify the Council of Management of any compliance failures that are material in their own right or as a pattern of failures.

If a staff member becomes aware of a data breach out of work hours they should advise their line manager immediately.

The Data Breach Report Form (appendix 4) should be completed following any breach.

4.9 Monitoring

Everyone must observe their policy. The Chief Executive has overall responsibility for the policy and will monitor it regularly to make sure it is being adhered to.

5 Failure to comply

We take the privacy of our staff, volunteers, clients and supporters seriously. Failure by staff and volunteers to comply with this policy may lead to disciplinary action.

Date of Draft	**July 2020**
Date of Implementation	**July 2020**
Date Reviewed	**June 2022 (Appendix 4 added)** **August 2022 reviewed by external consultant, DPO role allocated to Chief Executive**
Date of next review	**August 2023**

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 2018. 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 2013 (RIDDOR) (SI 2013/3163)
Accounting records	3 years for private companies, 6 years for public limited companies	Section 386 of the Companies Act 2006
Income tax and NI returns, income tax records and correspondence with the Inland Revenue	Not less than 6 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 2003 (SI 2003/2682)
Medical records and details of biological tests under the Control of Lead at Work Regulations 2002	40 years from the date of the last entry	The Control of Lead at Work Regulations 2002 (SI 2002/2676)
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) 2002	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 2002 (COSHH) (SI 2002/2677)

Records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 2002, 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 2002 (SI 2002/3006)
Records relating to the recruitment of employees	6 Months to 1 Year	None exist
Disclosure Barring Service (DBS) details	Disclosure number retained for period of employment	None exist
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	6 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	6 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	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

Appendix 2 – Data Protection Definitions

2.1 **'Data'** includes computerised and manual filing systems that are structured by reference to individuals and readily accessible, eg. card indexes, case file records.

2.2 **'Data controller'** is North Staffs Mind in its capacity as a collector of information, registered with the ICO. 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 with mental health issues.
- contact persons in external organisations
- 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.

Appendix 3 - Data Protection Policy

Adult Counselling Service - GDPR Consent

In accordance with the Data Protection Act 2018, GDPR, North Staffs Mind want to let you know about how we use your personal information.

- Personal information such as Name, Address, Date of Birth, Gender, Ethnicity, GP details are kept to process the referral into our service.

- Personal information, as detailed above, session attendance and evaluation records will be kept for 1 year (paper) and 6 years (electronically).

- Personal information and session attendance may be shared with 3rd parties such as GP's, Social Care agencies or NHS Access service on a need to know basis.

- Solicitors letters – We will send information on session attendance and evaluation scores only if we have written consent from you. We will not share what is discussed in sessions, this is in line with our Client Agreement.

- Letters for other purposes will be addressed to 'Whom it may concern' and given to you.

- North Staffs Mind is a Data Controller, meaning that we determine the processes to be used when using personal data. Our contact details are as follows: North Staffs Mind, 83 Marsh Street, Hanley, ST1 5HN. Tel: 01782 262100

- You have the right to do the following at any time:
    - Withdraw your consent for us to hold/process your data
    - Request a copy of the data we hold on you
    - Ask us not to share your information with a third party

  There will be no consequences to you for requesting any of the above. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so, for example, when there are risk or safeguarding concerns.

Please can you speak to your counsellor if you have any concerns regarding how we hold or use your information.

North Staffs Mind does not pass information onto anyone else for any other purposes.

Appendix 3A - Data Protection Policy

Younger Mind Client Consent Form

In accordance with the Data Protection Act 2018, North Staffs Mind wants to let you know about how we use your personal information. If you are under the age of 13, then the person with parental responsibility for you must sign this consent on your behalf.

• I understand that my personal information such as Name, Address, Date of Birth, Gender, Ethnicity, NHS Number, Parent/Carer, School and GP details are kept in order to process your referral to our service.

• I understand that when there is a Safeguarding or Child Protection concern my personal information, session totals and evaluation records will be kept until I reach the age of 18.

• I understand that, unless there is a Safeguarding or Child Protection concern as detailed above, my personal information, session totals and evaluation records will be kept for 1 year (paper) and 6 years (electronically).

• I understand that my personal information and session attendance information may be shared with 3rd parties such as GPs and Social Care agencies on a need-to-know basis.

• I understand that North Staffs Mind will submit my personal and session information and evaluation records to NHS England to be included in the Mental Health Service Data Set, which keeps track of the number of children and young people accessing counselling services in the UK.

• I understand that if I do NOT wish my data to be shared, then I am personally responsible for following the National Data Opt-Out procedure. You can find out information on how to do this at nhs.uk/your-data-matters

Signed:
Date Signed:
Relationship (if signing on behalf of Client):
Client Name:
Client Ref #:

APPENDIX 4 DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your manager immediately, complete Section 1 of this form and email it to itadmin@nsmind.org.uk.

Notification of Data Security Breach	**To be completed**
Date incident was discovered:	
Date of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident and details of the information lost:	[*Provide as much information as possible—including how the breach was discovered, the amount, sensitivity and type of data involved*]
Cause of the actual or suspected breach	[*Provide a detailed account of what happened*]
Is the actual or suspected breach ongoing?	[*Yes or No*]
Has any personal data been placed at risk? If, so please provide details:	
Number of Data Subjects affected, if known:	[*Include details of categories and approximate number of data subjects concerned*]
What are the likely consequences of the breach?	[*Consider the likely consequences for the affected data subjects*]
Brief description of any action taken or proposed to be taken, to deal with the personal data breach and, where appropriate, to mitigate any possible adverse effects:	[*Insert*]

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Data Protection Officer in consultation with the Head of area affected by the breach**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for Mind or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	

HIGH RISK personal data • **Sensitive personal data or special categories of personal data** (as defined in Data Protection Legislation) relating to a living, identifiable individual's: a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition; e) sex life or sexual orientation f) genetics g) biometrics, or h) commission or alleged commission of any offence. • **Criminal offence data**	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
Personal data relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	

Data Protection Officer to consider whether it should be escalated to the appropriate Mind SLT member	

Section 3: Action taken	**To be completed by Data Protection Officer**
Incident number:	
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	Yes/No If YES, notified on (date):
Follow up action required/recommended:	
Reported to Data Protection Officer on (date):	
Reported to other internal stakeholders (details, dates):	

For use of Data Protection Officer:	
Notification to ICO	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details: