



Headway North West London

Data Protection Policy and Procedure

The purpose of this policy is to enable Headway North West London (HNWL) to:

- Comply with the law in respect of the data it holds about individuals;
- Follow good practice;
- Protect Headway HNWL's staff, volunteers, members, service users and other individuals
- Protect Headway HNWL from the consequences of a breach of its responsibilities.

1. Legal Framework

Data Protection is important, not because it is about protecting data, but because it is about protecting people. People can be harmed if their data is misused, or if it gets into the wrong hands, through poor security or through careless disclosures. They can also be harmed if their data is inaccurate or insufficient and decisions are made about them, or about what services to provide to them on the basis of this data.

The Data Protection Act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act. The Act applies to *personal data* - information about identifiable living individuals that is:

- Held on computer or any other automated system
- Held in a *relevant filing system* (a paper system such as client records system, or a set of files on service users that is organized alphabetically by the name of the person or some other identifier such as case number)
- Intended to go onto computer or into a relevant filing system

2. Good practice principles

The Data Protection Act sets out eight enforceable principles of good practice. These principles are that the data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;

Data Protection Policy and Procedure	Version 3
Page 1 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019

- not kept for longer than is necessary;
- processed in accordance with individuals' rights;
- secure; not transferred to countries outside the EU without adequate protection.

3. Policy Statement

HNWL needs to collect, and use personal data (see paragraph below) about our service users, employees, volunteers and other individuals, who are referred to in the Act as “data subjects” in order to carry out our business effectively and provide high quality services. We hold information about data subjects for service provision, administrative, personnel management, and membership management purposes.

Sensitive personal data

The Act defines "sensitive personal data" as personal data consisting of information as to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life; the commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed, including the disposal of such proceedings or the sentence of any court in such proceedings.

The purpose for which we hold sensitive personal data about data subjects is for use solely for equal opportunities monitoring or for the provision of specific services to individuals. This includes but is not limited to: the provision of services to members and service users, assessing suitability and fitness for work, administering sick pay and sick leave, absence control, maternity leave and pay, parental leave, paternity leave and pay, adoption leave and pay, safe environment, complying with our obligations under the Disability Discrimination Act.

Statutory purposes

In addition to the purposes outlined above, we may collect, hold and process data including sensitive personal data if it is necessary to do so for compliance with any statutory duty with which we are required to comply.

Marketing activities

HNWL will also comply with the terms of the Act, and with other relevant legislations such as the Privacy and Electronic Communications (EC Directive) Regulations 2003, in relation to its marketing activities. Direct marketing refers not only to selling products and services to individuals, but also includes promotional activities. All individuals, without exception, have the right to prevent or stop their personal information being used for direct marketing. HNWL will state how personal information will be used and how individuals will be contacted.

Data Protection Policy and Procedure	Version 3
Page 2 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019

4. Related Headway policies/procedures, resources:

Confidentiality policy
Disclosure Information Policy and Procedure
Disciplinary Policy and Procedure
Record Keeping Policy and Procedure
Staff Handbook

Data Protection Procedure

The following procedure is designed to ensure that HNWL has mechanisms in place to ensure the principles of the Data Protection Act 1998 are adhered to. This section provides guidance to all staff and volunteers including trustees, on their obligations in respect of accessing, holding or using personal information during the course of their employment or volunteering, such as service user information and information relating to other members of staff or volunteers. It applies to all employees and volunteers. Those managing others should take particular notice of content, however, since they may have additional responsibilities under the Act.

HNWL will ensure that:

- there is someone with specific responsibility for data protection within the organisation
- all personal information collected will be factual and objective
- all those who manage and handle personal information understand the requirements of the Act and their responsibilities under it
- all those who manage and handle personal information are appropriately trained and supervised to do so
- the methods of handling personal information are regularly audited, reviewed and evaluated

Responsibilities

This policy applies to all staff, volunteers, Trustees and Management Committees. The procedure aims to set out the steps by which personal data is collected, the requirements to ensure records are completed appropriately and the requirements for the handling, storage and destruction of records.

The Trustees have overall responsibility for compliance with the Act, including registration and regular monitoring. The Trustees delegate compliance on a practical level insofar as service user information is concerned and compliance on all employee data as appropriate. (delete if no staff employed)

1.1 Senior Staff member/Trustees

Responsible for ensuring that all records are maintained and stored in accordance with the policy and procedure in place and adhered to. Also responsible for destruction of records in accordance with policy and procedure

Data Protection Policy and Procedure	Version 3
Page 3 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019

1.2 Staff

Responsible for compliance with the policy and procedure

2. Staff Responsibilities

2.1 Senior Person

To ensure that all staff, volunteers and service users have access to and are aware of this policy

To ensure that safeguards are in place to protect the interests of the service user.

2.2 All staff / volunteers / trustees

To be aware of and adhere to this policy and procedure.

The Act requires that all personal information is kept confidential and secure. You must therefore:

- observe all instructions or directions given to you in respect of confidentiality and security of information;
- comply with all security obligations under our Computer use and telecommunications Policy;
- comply with all confidentiality obligations contained within your employment/ volunteering contract;
- keep workstations locked when away from desks and keep any documentation containing personal information out of sight overnight, not left out on desks;
- inform the organisation of any changes to your personal details to enable us to comply with the Act and to aid the smooth running of the business;
- keep all lockable cabinets and drawers in which personal information is stored locked when not in use; and
- treat any documentation taken out of our offices in the same way as when in the office, ensuring security of information.
- Information held must be accurate, relevant and not excessive. If you need to hold or collect personal information you must therefore:
 - ensure that all documents containing personal information are up to date and held for no longer than is necessary; you should be aware that what constitutes “no longer than necessary” will vary and takes into consideration the type of information and the purpose to which it is to be put;
 - ensure that all documentation or other materials no longer required containing personal information are disposed of via secure destruction bins / shredders; and

Data Protection Policy and Procedure	Version 3
Page 4 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019

- ensure that the content of personal information held is objective; the information you hold may be disclosed to the individual concerned.

Staff /volunteers / trustees need to ensure that only the “authorised processing of information” takes place. In practice this means that:

- information held and used must be required by you in the information in the course of your employment or volunteering ; you must not access, gather or hold information which you do not genuinely need in order to carry out your role;
- access to personal information should be refused to individuals both internally and externally (without the consent of the data subject), unless it is clear that these individuals are authorised to access or process such information.

Except in certain limited circumstances, it is a criminal offence to obtain or disclose personal data or the information contained in personal data or to procure the disclosure of the information contained in personal data to another person without the consent of the person responsible for our compliance with the Act.

This means that:

- you may be committing a criminal offence if you do not process data in an authorised manner, whether you do so deliberately or because you have not taken sufficient care;
- you must comply with the terms of this Policy and with any further instructions or directions given to you;
- if you have any doubts or queries concerning your access to, or use of, personal data in the course of your employment or volunteering, you should seek guidance from your Co-ordinator [or any relevant Compliance officer].

2.3 Headway Staff / volunteer training

Staff responsible for the management of personal data must have had training in the provisions of the Data Protection Act 1998

All staff working with personal data need to be reminded that it is a disciplinary offence to disclose confidential information to unauthorised individuals

3. Audit Plan

The Co-ordinator/ senior person will monitor adherence of the policy and report findings to the Trustees.

Data Protection Policy and Procedure	Version 3
Page 5 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019

4. Third Parties

We do not normally have the need to provide information we retain on any of our staff, volunteers or service users to organisations or individuals outside HNWL other than to Social Services and other related statutory bodies during the course of client reviews and to any company which HNWL employs to undertake its administration processes. When we are asked to participate in client reviews, for referral purposes, or for any other reason we intend to pass information to another agency, we will always inform the client, volunteer or staff member of the information we intend to reveal and seek their agreement.

Data may also be disclosed to others at a data subject's own request.

5. Access and correction

The Data Protection Act 1998 gives individuals who are the subject of personal data a general right of access to the personal data which relates to them. For a copy of the information (to which the act applies) held about them an individual can write to:

The Board of Trustees
North West London Headway
C/O Thompsons Solicitors
Grove House
55 Lowlands Road
Harrow
HA1 3AP

HNWL reserves the right to charge the maximum fee payable in terms of the Data Protection Act for providing this information.

If the data held is inaccurate the individual is entitled to ask for it to be amended.

6. Retention of Data relating to employment or volunteering

We observe and abide by the Employment Practices Data Protection Code which is not enforceable by law but which provides guidance on best practice for employers in obtaining and processing information about employees

The categories of information which we will hold and the minimum time for which we will normally hold it will be as follows:

	Duration of Employment
Application Form	
References received	1 year
Payroll and tax information	6 years
Sickness records	3 years
Absence records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	5 years

Data Protection Policy and Procedure	Version 3
Page 6 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019

Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable reference to be provided	5 years from reference/end of employment
Summary of record of service e.g. name, position held, date of employment	10 years from end of employment
Records relating to accident or injury at work	12 years
Disclosure	CRB Guidance

The purpose for which we hold any information about data subjects after the end of employment (as indicated in the above table) is for use solely for any residual employment related matters including but not limited to the provision of job references, processing applications for re-employment, matters relating to retirement benefits and allowing us to fulfil contractual or statutory obligations.

7. Photographs

We will request consent before taking any photographs of individuals and will let them know how any photographs will be used.

8. Electronic communications

We monitor electronic communications by employees, volunteers and service users including to websites, to ensure that these systems are used in accordance with our internet policies.

9. Employee obligations

In the course of our business, we collect and process personal information, including that relating to service users, employees, contacts, and suppliers to which you may have access in the course of your employment. It is our policy to ensure compliance by our employees with the Act.

We reserve the right to implement the Disciplinary and dismissal Policy against anyone who fails to comply with the procedures set out in this policy and procedure.

10. References

Providing a reference involves the disclosure of personal data of the individual who is the subject of the reference. So that we can ensure we protect our employees' and volunteers data no references (whether to prospective employers or other institutions) should be given on behalf of the organisation without prior authorisation from the Senior person/trustees.

Data Protection Policy and Procedure	Version 3
Page 7 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019

This Policy does not prevent any employee giving a reference in a personal capacity but employees should make clear that such references are personal and not on behalf of the organisation and, if the reference is given on paper, that neither the organisation's name, address nor logo appear on the paper.

It is our policy to provide copies of references given by us to the individual who is the subject of the reference if they request a copy.

11. Marketing

We will inform individuals how and by whom their information will be used. This will include telling them that information may be shared with other organisations with similar aims and objectives such as Headway UK. When we collect information from people and are in direct contact with them such as in a phone call or via our website (delete as applicable) we will provide an immediate opportunity for them to opt out of further contact and to let us know how they would like to be contacted.

We will not make unsolicited **phone calls** to any organisation or individual who has told us they do not want our calls, or to any number on the Telephone Preference Service list.

We will not send unsolicited marketing by **electronic mail** to individuals without first getting their permission.

We will not send unsolicited **fax** marketing to anyone who has a number on the Fax Preference Service, or who has told us they object.

In all our marketing we will identify who we are and provide contact details, postal address, email address and free phone number so that the recipient can contact us. (If no delete free phone number available, insert contact telephone and state it is not free phone)

If an individual decides they no longer want to receive marketing, we will deal with their request promptly

12. Contacts for further advice on data protection

Information Commissioner's Office

Provide comprehensive information on the Data Protection Act and the legal requirements for compliance via web site www.ico.gov.uk and a helpline 08456 30 60 60 which is open between 9am and 5 pm Monday to Friday

Data Protection Policy and Procedure	Version 3
Page 8 of 8	Date of Approval 25 March 2017
	Revision date 25 March 2019