Data Protection

1. Introduction

1.1 Rationale

The Data Protection Act 1998 (DPA) regulates the way in which certain information about individuals is held and used.

Disability Equality NW recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

• keeping information securely in the right hands, and

• holding good quality information.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, DENW will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used (see separate document “Public Data Protection Statement”).

2.0 Purpose of the policy

The purpose of this policy is to enable Disability Equality NW to:

- comply with the law in respect of the data it holds about individuals;
- follow best practice;
- protect the rights of Disability Equality NWs' clients, Board Members, staff and volunteers.
- be open and honest with individuals whose data is held
- protect the organisation from the consequences of a breach of its responsibilities

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act.

3.0 This Policy Applies To

All staff, Board Members, Volunteers and those persons not directly employed by the organisation who may have legitimate access to data held by the organisation.

4.0 Accuracy of Data

It is recognised that data can at times be incorrect or out of date e.g. a change of address. All board members, staff and volunteers have a responsibility to ensure that the information held by DENW is correct and true. Where information recorded is found to be incorrect or out of date the record should be updated with the accurate information.

5.0 Security of Data

Disability Equality NW has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)

Adopted by DENW trustees at a meeting on 14/12/16

• Insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed

• Failure to offer choice about data use when appropriate

• Breach of security by allowing unauthorised access.

• Harm to individuals if personal data is not up to date

• Failure to offer choices about use of contact details for board members, staff, volunteers, and clients.

Each person authorised to access data held under the act is provided with their own log on and password, these details are to be kept secure and not to be shared or disclosed to another person or party unless directed to do so by their manager.

In order to maximise security passwords will be required to access:

• Organisation's network drives.

• Organisation's Email system

• The client database(s)

- The organisations Wi Fi (which will be split for internal and external users with both needing passwords to access).

It is good practice for passwords to be composed of a mixture of both alpha and numeric characters and should be changed periodically. If a board member, staff member or volunteer suspects that there may be a breach in data security or passwords, however trivial, they must report their suspicions immediately to their designated manager.

Paper records, other none electronic data, sensitive and confidential information must be kept securely with appropriate security measures in place with access restricted to appropriate persons only.

Any communications to be sent electronically to block of clients or members of the organisation must only be sent to recipients

as a blind copy (bcc) to ensure that information is sent to ‘undisclosed and contact details etc. are not accessible to unauthorised individuals.

Any documents containing data sensitive information (as per data protection training) which are sent via email should be double checked prior to being sent to ensure accuracy and should also be password protected.

The CEO and DENW board of trustees hold the following responsibilities:

• Briefing the board on Data Protection responsibilities

• Reviewing Data Protection and related policies

• Advising other staff on Data Protection issues

• Ensuring that Data Protection induction and training takes place

• Approving unusual or controversial disclosures of personal data

6.0 Use of Data and information

Information held on individuals is only to be accessed and used by staff, volunteers and board members in line with the Data Protection Act and in connection with the execution of their duties (see Data Protection: Storage and retrieval of information schedule).

7.0 Work Station and Paper Records Security

All authorised users are to ensure that any work station they are using is to be locked if the work station is left unattended in an area where data could be viewed by an unauthorised individual. Any paper records covered by the act should not be left in a place that would be accessible to unauthorised individuals.

8.0 Home Working and Remote Access.

This covers individuals accessing data when not on DENW premises.

Some individuals may be permitted to work from home, these individuals will be identified and authorised by the senior management team.

Whilst home working staff should ensure that access to their wireless connection is secure thus preventing unauthorised access to DENW via their network. During home working staff should take note of both this and the Lone/Home Working Policy.

When staff access the client database off site staff need to be mindful of the Work Station and Paper Records Security section 7.0 of this policy.

9.0 Staff Access to Information – Training

All board members, staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Any member of staff, volunteer, Board Member or other appropriately authorised party that has access to data covered by the act will receive data protection training during their induction and at any other time that the policy is updated to ensure the correct use and management of data in creating, accessing or processing personal information. Individuals will also receive training to enable them to understand their responsibilities under the Data Protection Legislation in respect of handling personal information.

Significant breaches of this policy will be handled under DENW's disciplinary procedures

10.0 Access to Information

Individuals who have data held about them have the right to see any data that identifies them or is specific to them as an individual.

Requests to access data are to be made in writing to the Data Protection Officer (CEO) in writing by the individual concerned or their recognised appointed representative.

Prior to providing information, the identity of the individual and their right to be provided with the information will be verified.

The required information will be provided in permanent form within 30 days from the request being received by the CEO.

Some individuals may find it difficult to communicate in writing, and may therefore have difficulty making a request to access information. DENW will make reasonable adjustments for such a person if they wish to make a request. Reasonable adjustments could include treating a verbal request for information as though it were a valid request. If the request is complex, it would be good practice for you to document it in an accessible format and to send it to the disabled person to confirm the details of the request. DENW will respond in a particular format that is accessible to the disabled person, such as Braille, large print, email or audio formats.

Staff should also take note of the following related policies

- Internet – acceptable use
- Lone /Home working Policy
- Email – acceptable use

  Data Protection statement and Storage of Data schedule

- Confidentiality Policy

11.0 Reporting Breaches of Data Protection Act

Adopted by DENW trustees at a meeting on 14/12/16

DENW is required to notify the Information Commissioner of the processing of personal data, this is included in a public register. The public register of data controllers is available on the Information Commissioner's website. Disability Equality NW's data controller's registration number is Z8950065. This should be on the certificate on the wall downstairs.

In the event that a member of staff feels that a breach of the Data Protection Act may have occurred, the incident must be reported immediately to the Chief Executive Officer.

Adopted by DENW trustees at a meeting on 14/12/16

DATA PROTECTION STATEMENT

Disability Equality (nw) Ltd. records personal information of any individual who makes an enquiry, or, accesses one of our services.

This is to keep accurate records, and to monitor our service. This information remains the property of Disability Equality (nw) Ltd. and will not be passed on to any other agencies without prior consent, unless determined by law.

We may occasionally contact you to evaluate our services. If you do not wishto be contacted in the future, please inform us, and the details of your enquiry will be destroyed after six months.

Adopted by DENW trustees at a meeting on 14/12/16

DATA PROTECTION: STORAGE OF PAPER and HARD COPY INFORMATION

Personal Information	Access to Information	Storage of Information
DE(nw) Employees & Trustees	CEO/Chair/Vice Chair	CEO Office & Safe
DE(nw) Volunteers	CEO/DfN Volunteer Co-ordinator (DFNVC)	Filing Cabinet by VBC desk (key in desk)
De(nw) Membership Details	CEO/Office Manager (OM)	Membership application forms to be stored in filing cabinets, key in desk
DE(nw) Clients	CEO/Information & Advice Service Manager (IASM)/Managed Accounts Manager (MAM)/LILS Manager (LILSSM)/ Hate Crime Reporting and Support Project Team Lead /Manager (DfNTL/CEO)	Enquiry sheets/files to be stored in filing cabinets, key in cupboard
Computers	Individuals to password protect own computers	List to be stored in safe
Clients requesting details	Proof of ID (photo ID if possible) to be produced before information is given	
Address Index Boxes (if used)	All Staff	To be stored in filing cabinet
Computer CD's & Disks	All Staff	To be stored in filing cabinet
Other organisations		Contact details to be stored in filing cabinet

Adopted by DENW trustees at a meeting on 14/12/16