

Wellspring Healthy Living Centre (WHLC Ltd)

DATA PROTECTION POLICY



Contents

1	Scope	3
2	Context	3
3	Purpose	3
4	Definition	3
5	Policy	4
6	Personnel/Employee Admin	4
7	Security	5
8	Contacts – collection of Data	5
9	Contacts – use of Data	6
10	Data Protection Checklist	7

1. SCOPE

This policy applies to all staff employed by the Company, those subcontracted by the Company and to all volunteers and casual workers and associated companies.

2. CONTEXT

The Data Protection Act 1998 requires the protection of personal data and all organisations which process personal data must be registered to do so. The Company is registered with the Data Protection Commissioner.

3. PURPOSE

This policy sets out an understanding of data protection and the requirements of every member of staff, sub contractor, volunteer or casual worker in order that there may be full compliance with the Data protection Act 1998.

4. DEFINITIONS

4.1 The Company is currently registered for six purposes:

- Accounts and Records
- Advertising, Marketing and Public Relations
- Staff Administration
- Administration of Membership Records
- Fundraising
- Realising the Objectives of a Charitable Organisation or Voluntary Body

4.2 Data is information which is recorded with the intention that it should be processed on computer or is recorded as part of a relevant filing system (i.e manual system). There are two categories of data:

4.2.1 Personal data is information relating to a living individual who can be identified:

- From the data
- From the data which includes an expression of opinion about the individual

Example: membership name and address details

4.2.2 Sensitive personal data is information relating to:

- Racial or ethnic origins of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health
- Sexual life
- The commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed or alleged to have been committed by the data subject

In order to process these types of data consent from the data subject must be obtained by the organisation handling the data. Explicit consent must be given when it is sensitive personal data.

5. POLICY

The Company has a data protection policy to ensure that it complies with all aspects of the data protection legislation (1984 and 1998) by setting out clear policies, responsibilities and codes of practice:

5.1 The Company intends to comply fully with all aspects of data protection legislation.

5.2 The Company will make all reasonable efforts to maintain a comprehensive written notification with the Data Commissioner.

5.3 The Company will do its utmost to ensure that all its staff, consultants and trustees are conversant with data protection legislation and practice.

5.4 The Company will only hold data for prescribed charitable purposes. These are personnel administration, accounts and records, advertising marketing and public relations, fundraising and charity objectives.

5.5 The Company will not pass personal data to third parties. This means that Wellspring will not sell/exchange its data to/within other organisations without prior consent.

5.6 The Company will use standard, approved statements about data protection in all the organisations literature in which personal data is collected. The statement for use is:

5.7 **“Data Protection Act 1998: The Company will only use personal data in connection with its charitable purposes. It does not make personal data available to any other organisation or individual without prior consent”.**

5.8 The Company will provide procedures for access to personal data for all those whom personal data is held. No charge should be levied on anyone (staff, personal members or other contacts) requesting access to their personal data. This will be reviewed if there is a high level of requests for access.

6. PERSONNEL/EMPLOYEE ADMINISTRATION

6.1 Personal and sensitive personal data are held on computer and in manual files at the Company. This data includes the following:

- Name, address and telephone
- National Insurance number and date of birth
- Nationality
- Bank details and details of any previous pension scheme
- Start date/ salary at start date
- Job title
- Emergency contact details
- Details of any regular medication

- Career history/previous employment
- Qualifications obtained/membership of professional bodies
- References
- Appraisals

6.2 Under the new legislation staff will be asked to sign a form consenting to data being held and processed for the following reasons:

- Recruitment and selection
- Performance management and training
- Absence recording
- Monitoring
- Statistical analysis

6.3 All staff may request sight of their personal details on computer provided reasonable notice (at least 14 days in writing) is given.

NB: references are exempt from all Data Protection legislation.

7. SECURITY

7.1 All personal and sensitive personal data held must be secure against unauthorised access and theft. Password protection is the most obvious means, but the server, filing cabinets and building in which the data is held must also be secure.

7.2 The Company needs to ensure that:

- Our IT network is as secure as possible from unauthorised access including access through the website.
- Individual PCs are password protected
- Individual PCs are logged off when individuals are away from their desk for more than ten minutes at a time.
- Personnel and other files holding sensitive or confidential personal data are secured and only made available to staff with authorised access.

7.3 Security on the Database.

The Database provides for different levels of security giving us the ability to ensure confidentiality of data by restricting access to different records and functions to only those users that need to use them. Please do not disclose your password to any other individual. Please log out when you do not need to use it and when you are away from your desk for a period of time (e.g. in a meeting or at lunch time).

8. CONTACTS: COLLECTION OF DATA

8.1 You have to make sure the Data Subject knows who you are and why and how the data will be used and that the data is relevant to the work of the Company.

- 8.2 If individuals are being added to the Company's database or manual filing system they need to be informed of how the Company will store and use their data at the time that the data is collected. This will require our Data Protection Act Statement to be included in all written requests for data. A verbal statement should be used for phone email or face to face collection. (These statement are not required if the manner in which the data is collected makes it obvious how it will be used, but will be necessary if the data may be used for other purposes).
- 8.3 The Company data protection statement must appear on all forms that people complete as a means of registering with the organisation, including those on the web. If they have not completed a form which includes the data protection statement then the statement must be included in a letter or email to the individual.
- 8.4 You have to get consent from the Data Subject to use their data, especially if it is sensitive data. i.e. covering racial or ethnic origin; religious or political beliefs, Trade Union Membership; Health; Sex Life; or Criminal Record.
- 8.5 When collecting emails addresses the Company's IT Policy must be used.

9. CONTACTS: USE OF DATA

- 9.1 Data, held by the Company, concerning any individual that enables that individual to be identified must not be given to any person outside the Company without the express permission of the individual concerned.
- 9.2 Do not reveal any sensitive personal data without the Data Subject's consent in writing or by email.
- 9.3 When using the email distribution lists send blind copies.
- 9.4 Check that you hold the data securely (use passwords on computer systems, don't leave files or screens visible, collect papers promptly from printers).
- 9.5 Consent must be obtained from the data subject if you are going to put personal data on the website.
- 9.6 The data must be accurate and you must have a good reason for using it.
- 9.7 You are only allowed to use data for the purpose which it was originally obtained. Data cannot be used for Direct Marketing, including fundraising, if the Data Subject requests you not to.

10 DATA PROTECTION CHECKLIST

10.1 Existing data

- Are you currently holding any personal data?
- Is it held securely?
- For what purpose are you holding it?
- Is it sensitive personal data?
- Does the individual know you are holding their personal data/ have they given their consent?
- Has the Company notified the Data Protection Commissioner that it holds this data and the purpose for which it is held? If not please tell the Centre Manager.
- Is the data accurate?
- Does the data still need to be held?

10.2 Collection of New Data

- Make sure you include the Company standard data protection statement on the form, together with a relevant opt out for other communications.
- When collecting data from new contacts by phone, email or letter, make sure they know about the data protection statement and IT policy.
- When requesting an article/page to be put on the website that will result in the collection of data ensure that a link is provided to the Company's Data Protection Statement and IT policy as appropriate.
- Check with the Centre Manager that the Company has notified the Data Protection Commissioner that this type of data is held
- Delete the data when it is no longer required
- Don't take personal data from another organisation without the consent of the individual concerned.

10.3 Use of Data

Are you passing personal data to anyone else:

- Inside the Company
- Outside the Company
- Are you using blind copies when sending email distribution lists?
- Is there a confidentiality agreement in place where it is necessary to pass data to a third party?

Do not pass personal data to any person outside of the Company without the permission of the individual to whom the data relates.