

DATA PROTECTION POLICY

1. POLICY STATEMENT

Wellspring is committed to a policy of protecting the rights and privacy of individuals (clients, staff [ie paid and voluntary office staff, cleaners, therapists, trainees] members of the Management Committee and others) in accordance with the Data Protection Act. Wellspring needs to process certain information about its clients, staff and other individuals it has dealings with for administrative purposes. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all clients, staff and Management Committee members of Wellspring. Any breach of the Data Protection Act 1998 or Wellspring's Data Protection Policy is considered to be an offence and in that event, Wellspring's disciplinary procedures will apply. Wellspring therapists who keep their own personal or process notes are expected to safeguard them in accordance with Data Protection legislation and to comply with this policy as regards records held by Wellspring.

2. BACKGROUND TO THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

3. DEFINITIONS (Data Protection Act 1998)

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.

Third Party

Any individual/organisation other than the data subject, the data controller (Wellspring) or its agents.

Relevant Filing System

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. **Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.**

4. RESPONSIBILITIES UNDER THE DATA PROTECTION ACT

- Wellspring is the data controller under the new Act.
- Compliance with data protection legislation is the responsibility of all members of Wellspring who process personal information.
- Staff and members of the Management Committee are responsible for ensuring that any personal data supplied to Wellspring are accurate and up-to-date.

5. NOTIFICATION

Notification is the responsibility of the Wellspring Administrator. Details of Wellspring's notification are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in Wellspring's Notification should seek advice from the Administrator.

6. DATA PROTECTION PRINCIPLES

All processing of personal data must be done in accordance with the eight data protection principles.

1. **Personal data shall be processed fairly and lawfully.**
Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**
Data obtained for specified purposes must not be used for a purpose that differs from those.
3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**
Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
4. **Personal data shall be accurate and, where necessary, kept up to date.**
Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by Wellspring are accurate and up-to-date.
5. **Personal data shall be kept only for as long as necessary (see Section 12 on Retention and Disposal of Data).**
6. **Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act (see Section 7 on Data Subjects Rights).**
7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. (see Section 9 on Security of Data)**
8. **Personal data shall not be transferred to a country or a territory**

outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data must not be transferred outside of the European Economic Area (EEA) - the fifteen EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. It should be remembered that information published on the Internet can be accessed from anywhere in the globe.

7. DATA SUBJECT RIGHTS

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

8. CONSENT

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. Wellspring understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by Wellspring (eg when a client signs the consent section of the

Application Form or when a member of staff signs a contract of employment or Agreement of Association). Any Wellspring forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

If an individual does not consent to certain types of processing, appropriate action must be taken to ensure that the processing does not take place.

9. SECURITY OF DATA

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party (see Section 11 on Disclosure of Data for more detail).

All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised persons.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside Wellspring.

10. RIGHTS OF ACCESS TO DATA

Members of Wellspring have the right to access any personal data which are held by Wellspring in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by Wellspring about that person. Wellspring clients also

have the right to access any personal data held by Wellspring in electronic format and manual records forming part of a relevant filing system.

Any individual who wishes to exercise this right should apply in writing to the Administrator. Wellspring reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. See Subject Access Request Procedure.

11. DISCLOSURE OF DATA

Wellspring must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (eg a client or staff member has consented to Wellspring corresponding with a named third party);
2. where the disclosure is in the legitimate interests of Wellspring (eg disclosure to staff - personal information can be disclosed to other Wellspring staff members if it is clear that they require the information to enable them to perform their jobs);
3. where Wellspring is legally obliged to disclose the data;
4. where disclosure of data is required for the performance of a contract (eg informing a funder of a client's non-attendance at sessions).

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security*;
- prevention or detection of crime including the apprehension or prosecution of offenders*;
- assessment or collection of tax duty*;
- discharge of regulatory functions (includes health, safety and welfare of persons at work)*;
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member or client of Wellspring, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (ie consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member or client of Wellspring may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, Wellspring may offer to do one of the following:

- pass a message to the data subject asking them to contact the enquirer;
- accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: ie "if the person is a member/client of Wellspring" to avoid confirming their membership of, their presence in or their absence from the organisation.

12. RETENTION AND DISPOSAL OF DATA

Wellspring discourages the retention of personal data for longer than they are required. Once a member of staff has left Wellspring, or a client has ended therapy, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Clients

Information held on individual clients should be regularly reviewed in accordance with Wellspring's Procedures for Data Handling and Storage.

Staff

Information on individual members of staff will be retained after they have left Wellspring only when deemed appropriate and will be destroyed whenever their usefulness expires.

The personal files of individual staff members should be regularly reviewed in accordance with Wellspring's Procedures for Data Handling and Storage.

Information relating to unsuccessful applicants in connection with recruitment to a post will be kept for 12 months from the interview date. A record of names

of individuals who have applied for, been short-listed or interviewed for posts may be kept indefinitely.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).