Data Protection Policy

(Revised to comply with GDPR May 2018)

Aims and Scope of the Policy:

The purpose of this policy is to set out Wellspring Healthy Living Centre's (WHLC) commitment and procedures for protecting personal data. We regard the lawful and correct processing of personal information as essential to our work and important in maintaining the confidence of those whom we exist to support.

This policy has informed our Privacy Statement which is set out in Appendix 1 and the Procedures for handling data and data security, which are set out in Appendix 2.

All staff and freelance workers are required to sign that they have read this policy and agree to abide by our procedures.

1. **Legal framework:**

Data Protection Act 1998 – this is the UK legislation that provides the framework for responsible behaviour for those using personal information. It was replaced by the General Data Protection Regulation (GDPR) on 25 May 2018.

GDPR extends the duties of any organisation or individual (e.g. sole trader) who uses personal data (such as name, contact information, employment information) that relates to a known, living human being. The regulations have been devised to take into account how electronic data and the internet are being used in practice. GDPR aims to give control back to citizens and residents over their personal data and provides citizens with new rights.

Information Commissioners Office (ICO) is the Data Protection regulator. Its job is to uphold information rights in the public interest.

2. **Does GDPR apply to our organisation?**

GDPR applies to anyone who controls, uses or works with data. These definitions are similar to those under the existing Data Protection Act (DPA); a controller is the person, people or organisation who decides how and why personal data is stored and used; whereas the processor is a person, persons or organisation who acts on their behalf. Both a controller and processor can be a legal entity (for example a VCSE organisation or business) or natural person (an individual) and are often both. For example, an organisation which collects information about service users and analyses it for their internal monitoring would be both a controller and processor.

3. **How do we know if the data we hold is covered by GDPR? What is 'personal data'?**

The regulations cover everything that could be classed as personal data, both electronic and manual filing systems. People have the right to know who is storing their data, why the information is being

kept and how it will be used. Importantly, they also have a right to have access to their personal data. Personal data is any information which could identify a living individual (including an Internet Provider (IP) address which identifies individual computers). This is broader than under the existing DPA regulations. The following are considered personal data (this list is not exhaustive):

- Name
- Home address
- Email address
- Phone number
- Computer IP address
- Job title
- Photograph
- Work email if it obviously directs to a particular person eg: elaine.flint@wellspringhlc.org
- Work mobile telephone if it goes to the same individual (NOT an office telephone if that could go to several people.)

4. What is data processing?

Data processing is a broad term which covers the obtaining, recording, holding and carrying out operations or analysis of information or data. Generally, this includes: adapting, altering, combining, destroying, disclosing, organising, recording or using data. Some examples of data processing are:

- Keeping a mailing list of contacts which you periodically contact via email, post, phone;
- Storing information about historical donors to your organisation (so you can contact them again in the future);
- Keeping names and addresses of people who've used your services in the past (i.e. for monitoring and reporting purposes) or are members of your group/organisation.

5. What is our lawful basis for the processing we do?

GDPR says that before processing personal data you need to establish a lawful basis for processing the information. The main legal basis is likely to be having consent from the individual. In some instances, it is possible to use legitimate interest as the lawful basis. Other foundations for processing include situations where processing is necessary to:

- Perform a contract entered into with the data subject;
- Comply with a legal obligation;
- Protect the vital interests of a data subject or another person;
- Perform a task in the public interest or to exercise an official authority vested in the controller.

6. Data collection and informed consent:

We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person or by completing a form, for example through the website.

When collecting data, we will ensure that the Data Subject:
Clearly understands why the information is needed and
Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing.

7. Applying legislation within WHLC

WHLC is the data controller and is therefore legally responsible for complying with GDPR, which means that it determines what purposes personal information held will be used for.

WHLC will take into account legal requirements and ensure it is properly implemented and, through appropriate management, apply strict application of criteria and controls.

The data retention periods contained in other legislation and through best practice that we apply is set out in Appendix 3.

8.Responsibility for Data Protection at Wellspring

The designated data protection officer for WHLC is the Chief Executive Officer. It is however the responsibility of all staff who process or have access to personal information to ensure that the GDPR principles are followed and fully implemented. Any breaches of Data Protection Policy must be reported to the Chief Executive Officer using the Information breach incident reporting form (also see Incident management procedures: Information breach).

All staff, including freelance contractors and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them, in accordance with WHLC's Disciplinary Procedure.

WHLC's Confidentiality Agreement sets out important guidance to staff for the security of confidential information to meet GDPR principles.

9. Data Subject Access Requests

WHLC recognizes that as a data controller, we much uphold an individual's rights to access their personal data. We also recognize an individual's rights to data portability which only applies:
To personal data an individual has provided to a controller
Where the processing is based on the individual's consent or for the performance of a contract and
When processing is carried out by automated means.

We endeavor to process such request as soon as possible and within one month from receipt of the original request. The request must be in writing.

10. Checking identity

To protect the confidentiality of information, we verify the identity of anyone before proceeding with any request made towards WHLC in regards to an individual's own data. Any request by a third party needs to be accompanied by adequate proof that the individual in question has given clear authority to that third party to act on their behalf.

11. Disclosure

We may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The data subject will be made aware in most circumstances how and with whom their data will be shared. There are circumstances where the law allows for the charity to disclose data (including sensitive data) without the data subject's consent. These are:

Carrying out a legal duty or as authorized by the Secretary of State, protecting the vital interests of a data subject or another person.
The data subject has already made the information public.
Conducting legal proceedings, obtaining legal advice or defending any legal rights.
Monitoring for equal opportunities purposes – ie race, disability, religion.
Providing a confidential service where the data subject's consent cannot be obtained or where it would be reasonable to proceed without consent eg where we would wish to avoid forcing stressed or ill data subjects to provide consent signatures.

12 Data breach

This policy is designed to mitigate and scope for data breaches, however WHLC will meet its obligations to the ICO to ensure any data incident is effectively managed, appropriately investigated and reported where necessary.
See WHLC's Information Incident Management Procedures and Information Incident Breach Reporting Form.

Agreement (staff, freelance workers and volunteers)

WHLC expects all those who work on WHLC's behalf to comply fully with this Policy and the Principles of the General Date Protection Regulation.
Disciplinary action may be taken against anyone who breaches any of the instructions or procedures in this policy.

Please sign to confirm your acceptance and understanding of this policy.

Name:

Signed:

Date:

Appendix 1.

Your right to privacy - Wellspring Healthy Living Centre

Who we are?
We are Wellspring Healthy Living Centre, a charity dedicated to improving the health of the local community within Lawrence Hill, Easton and the surrounding areas. Wellspring HLC is a registered charity whose number is 1134593 and a limited company whose number is 6040773. The registered address is Wellspring Healthy Living Centre, Beam Street, Bristol BS5 9QY.

What is GDPR?
GDPR covers any information that can be classified as personal details or information that can be used to identify you, and covers a range of information including:

- Name
- Photo/cctv images
- Email/ IP addresses
- Social media posts
- Personal medical or social care needs information

Wellspring HLC is serious about protecting your privacy and storing your data securely. New legislation now exists which states what obligations we have to follow when collecting and storing your data, it's called General Data Protection Regulations (GDPR). These are the rules that govern how we collect, store and use personal data. It is possible you've had a number of emails or letters about it from other people who hold your personal data. All information is treated with the highest standards of confidentiality and security.

How we collect information from you?
We obtain your information when you use our services or attend one of our sessions, we will advise you of our policy and ask you to sign a consent form. If you give us verbal consent we will also ask you to sign a consent form.

Why is this information being collected?
- Wellspring collect information to:
- Keep you updated about the service you are using.
- To monitor who uses our services and who doesn't.
- To signpost you to other services that you are interested in.

What type of information is collected from you?
Contact information: When you contact us we collect your name, address, telephone and email contact. We use this information to contact you regarding our services. We will not share this information with any third party unless you give us explicit consent or there are safeguarding concerns.

Sensitive personal data: We ask you to provide sensitive data about your specific interests. We will not share this information with any third party unless you give us explicit consent or there are safeguarding concerns.

Monitoring information: We ask that you complete an anonymous equalities monitoring form that is classed as sensitive personal data. We will not share this data in a way that you could be identified. This data will be used to evaluate services or update funders in an anonymised format.

Where is your information kept?
Your information is kept on password protected digital systems and daily backups are made and held in a GDPR compliant cloud.

Paper records are kept in a locked filing cupboard and are destroyed when updated to a digital system or destroyed six years after finishing a service.

All mobile systems will hold limited details and will be password protected.

Who has access to your information?
Only relevant staff of Wellspring HLC can access your detail.

How can you delete your data?
At any point you can choose to stop having your data stored by Wellspring HLC. All you need to do is email us on info@wellspringhlc.org and ask us to “Delete my data”

How you can access and update your information?
By using our services, you are agreeing to be bound by this policy, however if you have any queries in regards to this policy please contact us by emailing: info@wellspringhlc.org or write to us at Wellspring HLC at Beam Street, Bristol BS5 9QY. Alternatively you can telephone 0117 3041400.

Appendix 2: Procedures for handling data and data security

Phone calls:

Make sure that any phone calls you make that contain personal information are made from settings where they cannot e overheard by the general public

Before leaving a message consider the urgency of getting the information to the client. If it is not urgent and another attempt to speak to the client can be made, do not leave a message.

If you feel you have to leave a message, think about what you say, and leave the minimum amount of information –for example, 'Please call (number) to talk about your appointment'

When the phone is answered by someone else:

Always ask to speak to the client, but don't say where you are calling from initially. If they ask who is calling, you should respond with a minimum amount of information. Stating you are calling about their appointment may be sufficient.

If the client is not present, then unless there is a degree of urgency do not leave a message, but ask when is a good time to call back.

If the client is present but unable to speak (either due to language or physical difficulties), ask to speak to the next of kin. Before giving information to them, try to ascertain whether they are aware of why you may be calling (it may be necessary to reveal basic information to do this)

Check that the person you are talking to is the client. It may help to start the conversation with "This is Wellspring Healthy Living Centre, please can you let me know who I am speaking to."

Personal information should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

Email:

Always remember that emails can go astray – do not put personal information about clients in the body of emails. If personal information needs to be transmitted – for example to freelance therapists/artists, they need to be attached as passworded excel files with the password sent in a separate email.

Group emails should be blind-copied (bcc) if they contain any personal email addresses unrelated to work roles.

Emails that contain personal information which is no longer required for operational use should be deleted from the personal mailbox and any "deleted items" box.

Consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder on the data network and deleted from the email inbox.

Data security and storage

Store as little personal data as possible on your computer of laptop. Only keep those files that are essential. Personal data received on memory stick should be saved to the relevant file on the data network.

Ensure that PCs and laptops are locked or logged off when you are away from your desk. This is particularly important when using your laptop away from the office.

Paper files holding personal or sensitive personal data must be secured and only made available to staff with authorised access.

If you are working from paper forms on your desk with personal information, ensure that you turn them over to protect them from the view general public or put them in a cardboard document wallet if disturbed by a member of the public entering the office.

If you have the database with personal information up on your screen when a member of the public enters the office, minimise it so it isn't visible.

When away from the building, make sure that personal data on paper files is secured in locked cases when in transit outside the office and treated in the same way as for laptops (below). A spare lockable case is available in Room 28 for those who do not need regular use of this facility.

Laptops and portable devices:

All portable devices including laptops, mobile phones and all devices used to access WHLC data should be password or PIN protected.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended when in public venues away from the office. When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Protect your password – do not keep it written on something stored in the laptop case.

Public conversations:

Wellspring is a public building with many community users. Please be aware that conversations can be overheard and confidential information inadvertently disclosed. Ensure conversations about clients take place in private spaces.

Paper storage and disposal

Use the confidential waste unit in the photocopier room to dispose of all paper material that contains sensitive information.

Ensure that all files containing personal sensitive information are kept in locked units and are only kept for the length of time required. Where possible scan information onto the network and onto the database.

APPENDIX 3 INFORMATION RETENTION SCHEDULE

Type of record	Retained for:	Why retained
Employee information	6 years from the termination of employment Legal basis: Section 5 Limitation Act 1980	The purpose for which WHLC holds any information about Employees after the end of employment is for use solely in relation to residual employment related matters including, but not limited to; the provision of job references, processing applications for re-employment, matters relating to retirement benefits, the fulfilment of contractual or statutory obligations.
Job candidate information	6 months	The records of unsuccessful job applicants will be kept for 6 months. This allows for revisit if the recruitment is unsuccessful and also for challenge of the recruitment process.
Finance records	6 years	Section 338(4)(a)(b) Companies Act 2006
Board meeting minutes and resolutions	10 years from the date of the meeting	Section 248 Companies Act 2006
Volunteers	2 years from date of last contact	This will allow for references to be provided (if applicable) and for funding reporting.
Contracts, agreements and other arrangements	For the length of the contract or agreement and 6 years afterwards	Section 5 Limitation Act 1980
Insurance policies	Employers Liability policies are required to	Employers' Liability (Compulsory Insurance) Act 1969

	be retained for a minimum of 40 years	
Accident reports	Minimum 3 years	Reg 12, RIDDOR 2013
Mental Health Service Clients (IAPT)	20 years	As per best practice set out in our contract with the NHS
Community Groups / class attendees	6 years from date of last contact	Section 5 Limitation Act 1980
Smoking Cessation	2 years from date of last contact	As per NHS best practice
CHC clients (musculoskeletal)	8 years from date of last contact	Best practice retention of health records from the Chartered Society of Physiotherapists
Clients who are children or young people when attending Wellspring	Until the client's 25th birthday or 26th if young person was 17 at conclusion of treatment, or 8 years after death.	NHS best practice