DATA PROTECTION POLICY

This Policy has been approved & authorised by:

Name: **Mark Swift**

Position: **CEO**

Date: **23/11/23**

Signature: 

This Policy has been approved & countersigned by:

Name: **Tim Phillips**

Position: **Director**

Date: **23/11/23**

Signature: 

Policy last reviewed on: 22/11/2023

Policy last reviewed by: RP

Policy next due for review: 22/11/2024

Wellbeing Enterprises CIC
Bridgewater House
Old Coach Road
Runcorn
WA7 1QT

t: 01928 589799
e: info@wellbeingenterprises.org.uk

HUMAN RESOURCES POLICY TRACKING SHEET

Amendment	Reason for amendment	Date
Policy Reviewed	ICO ref updated page 15	23/10/2019
	IDPO and Data Protection leads names removed from Policy and Mark Swift added (pg5,6 & 15)	*08/11/19*
Policy Reviewed	*List data shared with amended page 9; Happy Place App mentions removed, page 5, 6, 7 and 9; formatting pages 27 and 28*	*10/02/2021*
Policy Amendment	*Phone and device section 12 Password complexity section 13*	*03/06/2021*
Policy Amendment	*Formatting chapter order 11,12, 13; Following sections have been edited, data we collect, how and why we use data, who we share data with, sharing with third parties, security measures, DPIA.*	*08/12/2021*
Policy Amendment	*Rewritten to remove Privacy Notice material and focus directly on data protection issues*	*22/12/2021*
Policy review	*No Amendments*	*25/01/2023*
Policy Review	*No Amendments*	*22/11/2023*

Data Protection Policy

1. Context & Overview

1.1 Introduction

Wellbeing Enterprises was established in 2005 as the first Wellbeing Community Interest Company in the UK.

Wellbeing Enterprises needs to gather and use certain personal information about the clients that it provides products and services to. Additionally, the Organisation may hold personal information on: employees, suppliers, and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Organisation's data protection standards – and to comply with the law.

1.2 Data Protection law

The UK General Data Protection Regulation (GDPR) 2021 and the Data Protection Act 2018 require that data about individuals (personal data) are collected only for specified, explicit and legitimate purposes, are adequate, relevant and limited to what is necessary for those purposes and are accurate and, where necessary, kept up to date. They should be kept in a form which permits identification of data subjects for no longer than is necessary and must be processed in a manner that ensures appropriate security.

Furthermore the data must be processed lawfully and with a clear legal basis and the processing must be fair and transparent to the individual data subjects concerned. The law provides individuals with a range of rights which must be respected.

Wellbeing Enterprises CIC is responsible for, and must be able to demonstrate, compliance with the Principles set out above and breaches may result in significant fines and

1.3 Policy scope

This policy applies to:

- All staff of Wellbeing Enterprises CIC
- All contractors, suppliers and other people working on behalf of Wellbeing Enterprises CIC

It applies to all data that the company holds relating to identifiable individuals, in our case patients and staff. This information can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to an individual; for example, treatment being undertaken, who can be identified from that information either directly or when the information is combined with other existing information

2. Who? People and responsibilities

Everyone at Wellbeing Enterprises CIC contributes to compliance with GDPR. Key decision makers must understand the requirements and accountability of the organisation sufficiently to prioritise and support the implementation of compliance.

The **board of directors** is ultimately responsible for ensuring that Wellbeing Enterprises CIC meets its legal obligations. **Tim Phillips, Board Director**, is Executive Lead for compliance.

The **CEO, Mark Swift**, m.swift@wellbeingenterprises.org.uk is responsible for:

- Keeping senior management and board updated about data protection issues, risks and responsibilities
- Documenting, maintaining and developing the organisation's Information Security and Data Protection policies and related procedures, in line with an agreed schedule and disseminating policy across the organisation, and arranging training and advice for staff.

- Ensuring that Data Protection Impact Assessments are undertaken prior to all new developments or changes to the way that personal data are processed and that all new work incorporates Privacy by Design principles.
- Checking and approving contracts or agreements with third parties that may handle the company's sensitive data and evaluating any third party services the company is considering using to store or process data, to ensure their compliance with obligations under the regulations.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards and performing regular checks and scans to ensure security hardware and software is functioning properly.
- Developing privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the companies use of their data
- Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles

Data Protection Officer – Mark also fulfils the responsibilities of the DPO in respect of Wellbeing Enterprises. The DPO is responsible for:

- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- Being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, clients etc)

All Staff should keep all data secure, by taking sensible precautions and complying with our Security Policy including:

- Strong passwords must be used and never shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data must not be shared informally.
- When access to areas containing sensitive data is required, this must be requested and approved by an individual's line manager.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required it should be deleted and disposed of. In any event patient data should not be retained beyond 8 years.
- Employees should request help from their line manager should they be unsure about any aspects of data protection.

3. How we meet our Data Protection Responsibilities

3.1 Data Privacy Impact Assessments (DPIA)

Wellbeing Enterprises conducts Data Privacy Impact Assessments prior to the implementation of any new system or process which has the potential to impact the data we collect and store. This enables us to identify the most effective ways in which to comply with our data protection obligations while continuing to meet clients' expectations of privacy and protect against the risk of harm through use or misuse of personal information. When conducting a DPIA we assess:

- The purpose of the processing operations and the legal basis for processing, including the common law of confidentiality and other information law
- The necessity and proportionality of the processing in relation to the purpose.
- The risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.

3.2 Privacy by Design

Privacy by Design is an important concept within the UK GDPR and promoted by the UK Information Commissioner. It is essential that IT solutions and software are developed with Privacy by Design principles in mind and Wellbeing Enterprises CIC aims to ensure that it follows recognised best practice. More detail can be found in Appendix 1.

3.3 Information Security

We know how much data security matters to all of our clients. With this in mind, we will treat your data with the utmost care and take all appropriate steps to protect it.

We secure access to all transactional areas of our website using 'https' and 'SSL' technology. Usernames and passwords are stored in an API database and Passwords are hashed so that they are unreadable. The user table is encrypted so it is unreadable without access via a client application. Access is only available to those with certificate access to the server.

Google Analytics is committed to GDPR and the protection of the data it stores. Google Analytics is ISO 27001 accredited. Further information regarding how Google Analytics safeguards your data can be found here.

Access to your electronic personal data is restricted, secure password admission is required. We use secure certificates (SSL) to ensure data is encrypted in transit. The data is stored in a secure SQL Server database with a certified provider. Our system is role based. We only store minimum data for the service.

Copies of paper based personal information is locked away securely in our filing systems and does not leave the premises

We regularly monitor our system for possible vulnerabilities and attacks, and we carry out penetration testing to identify ways to further strengthen security.

We secure access to our Welljoy shop website using https and the transmission of sensitive payment information through designated purchase forms protected by SSL / TLS encrypted connection, regularly maintain a PCI DSS (Payment Card Industry Data Security Standards) certification.

More detail on our security is set out in our Information Security Policy.

3.4 Privacy Notice

Wellbeing Enterprises aims to ensure that individuals are aware that their data is being processed, and that they understand:

- Who is processing their data
- What data is involved
- The purpose for processing that data
- How to exercise their rights

To these ends the Organisation has a Privacy Notice, setting out how data relating to these individuals is used by the company. The Privacy Notice can be viewed online http://wellbeingenterprises.org.uk/terms-and-privacy-policy/

4. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance is an ongoing process. Wellbeing Enterprises have implemented the following measures to ensure ongoing compliance:

1. Maintain documentation/evidence of the privacy measures implemented and records of compliance.
2. Manage Data Protection Impact Assessments as living and evolving documents to ensure that they accurately reflect current practice.
3. Regularly test the privacy measures implemented and maintain records of the testing and outcomes.
4. Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.
5. Keep records showing training of employees on privacy and data protection matters.
6. ICO registration renewed annually. Current registration number is: Z9945371

Appendix 1

Privacy by Design

The principles are set out below

	Privacy by Design Principles	Privacy – Respect and protect personal information	Security – Enable and protect activities and assets of both people and enterprises
1	Proactive not Reactive. Preventative, not Remedial	Anticipate and prevent privacy-invasive events before they happen. Don't wait for privacy risks to materialise.	Begin with the end in mind. Leverage enterprise architecture methods to guide the proactive implementation of security.
2	Default Setting	Build privacy measures directly into any given ICT system or business practice, by default.	Implement 'Secure by Default' policies including least privilege, need to know, least trust, mandatory access control and separation of duties.
3	Embedded into Design	Embed privacy into the design and architecture of ICT systems and business practices. Do not bolt it on after the fact.	Apply Software Security Assurance practices. Use hardware solutions such as Trusted Platform Module.
4	Positive-Sum, not Zero-Sum	Accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a zero-sum approach involving unnecessary trade-offs.	Accommodate all stakeholders. Resolve conflicts to seek win-win.
5	End-to-End Security	Ensure cradle-to-grave, secure life cycle management of information, end-to end.	Ensure confidentiality, integrity and availability of all information for all stakeholders.
6	Visibility and Transparency	Keep component parts of IT systems and operations of business practices visible and transparent, to users and providers alike.	Strengthen security through open standards, well known processes and external validation
7	Respect for the User	Respect and protect the interests of the individual, above all. Keep it user-centric.	Respect and protect the interests of all information owners. Security must accommodate both individual and enterprise interests.