DATA PROTECTION POLICY

This Policy has been approved & authorised by:

Name: **Mark Swift**

Position: **CEO**

Date: **10/06/2021**

Signature: 

This Policy has been approved & countersigned by:

Name: **Tim Phillips**

Position: **Director**

Date: **10/06/2021**

Signature: 

Policy last reviewed on: 10/02/21

Policy last reviewed by: RP

Policy next due for review: 10/02/22

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

t: 01928 589799
f: 01928 551 922
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*

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.

For simplicity throughout this notice, 'we' and 'us' means Wellbeing Enterprises.

1.2 Why this policy exists:

This Data Protection policy ensures Wellbeing Enterprises CIC:

- Complies with data protection law and follows good practice
- Protects the rights of clients, staff and partners
- Is transparent about how it stores and processes individuals' personal data
- Protects itself from the risks of a data breach

1.3 Data Protection law:

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from 25th May 2018. It states that personal data shall be:

1. *Processed lawfully, fairly and in a transparent manner in relation to individuals.*

2. *Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes.*

3. *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

4. *Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

5. *Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals.*

6. *Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

7. *The Controller shall be responsible for, and be able to demonstrate, compliance with the Principles.*

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**, is responsible for:

These responsibilities should include (but are not necessarily limited to):

1. Keeping senior management and board updated about data protection issues, risks and responsibilities

2. Documenting, maintaining and developing the organisation's Data Protection policy and related procedures, in line with agreed schedule

3. Embedding ongoing privacy measures into corporate policies and day-to-day activities, throughout the organisation and within each business unit that processes personal data. The policies themselves will stand as proof of compliance.

4. Dissemination of policy across the organisation, and arranging training and advice for staff

5. Dealing with Subject Access Requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters

6. Checking and approving contracts or agreements with third parties that may handle the company's sensitive data

7. Ensuring all systems, services and equipment used for storing data meet acceptable security standards

8. Performing regular checks and scans to ensure security hardware and software is functioning properly

9. Evaluating any third party services the company is considering using to store or process data, to ensure their compliance with obligations under the regulations

10. 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

11. Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles

Informal Data Protection Lead – the person responsible for fulfilling the tasks of the DPO in respect of Wellbeing Enterprises is:

Name: Mark Swift

Job Title: CEO

Email: m.swift@wellbeingenterprises.org.uk

Under GDPR, organisations in certain circumstances are obliged to appoint a DPO. Currently, Wellbeing Enterprises CIC does not meet the criteria to appoint a formal DPO, however we are committed to best practice so have appointed an Informal DPO to lead on ensuring that data protection obligations are met.

The IDPO is responsible for:

- *Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws*

- *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)*

3. Scope of personal information to be processed

3.1 When do we collect your personal data?

We collect your personal information in a number of ways:

- Referral form (when an individual first comes in contact with our services)
- Via our website through the booking form system, subscribing to email newsletters, and 'Contact Us' form
- Questionnaires when first accessing our services
- When completing a purchase on the Welljoy Shop

3.2 What sort of personal data do we collect?

We collect the following personal information:

- Name
- Gender
- Date of Birth
- Address
- Email
- Telephone
- Copies of documents provided by third parties e.g. medical records
- Information gathered by the use of cookies in your web browser
- Information gathered by Google Analytics

3.3 Uses and conditions for processing

The General Data Protection Regulation sets out a number of different reasons for which an organisation may collect and process your data. These include:

Consent
In specific situations, we can collect and process your data with your consent.
When collecting your personal data, we'll always make clear to you which data is necessary in condition with a particular service.

Contractual obligations
In certain circumstances, we need your personal data to comply with our contractual obligations.

Legal compliance
If the law requires us to, we may need to collect and process your data.

Legitimate interest
In specific situations, we require your data to pursue our legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact your rights, freedom or interests.

3.4 How and why do we use your personal data?

We collect this information for the following purposes:

- To protect our organisation and you from fraud and other illegal activities. (Legal compliance)
- To comply with our contractual or legal obligations to share data with law enforcement. (Legal compliance)
- To supply anonymised data to the commissioners who fund us to demonstrate the work we have delivered. (Contractual obligation)
- To send you email newsletters about our services. (Consent)
- To send you communications required by law or which are necessary to inform you about our changes to the services we provide to you. For example, updates to this Privacy Notice. These service messages do not require prior consent when sent by email or text message. If we do not use your personal data for these purposes, we would be unable to comply with our legal obligations. (Legitimate interest)
- To enhance, modify, and improve the services we deliver to the community. (Legitimate interest)
- To participate in research studies to evidence the benefits our service has on the people and communities it supports. (Your information will not be shared for this purpose without your consent). (Legitimate interest)

Outcome/Use	**Processing required**	**Data to be processed**	**Conditions for processing**	**Evidence for lawful basis**
Referral form	*Electronic sent Via email*	*Name DOB Address GP Practice Telephone number Ethnicity*	*Legitimate interest*	*Evidence of date of verbal consent given*
Questionnaire	*Paper copy transferred to electronic data management system*	*Name Gender Email Post Code GP Practice Employment Status*	*Consent*	*Evidence of consent given via questionnaire*
Online booking form	*Electronic via website*	*Name Email Address Telephone number*	*Legitimate interest*	*Privacy terms available on website www.wellbeingenterprises.org.uk*
Welljoy Shop Checkout	*Electronic via website*	*Name Address Postcode Email Telephone Number*	*Legitimate interest*	*Privacy terms available on website www.weljoyshop.co.uk*

4. 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 legitimate interests pursued by the Controller.
- 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.

See Appendix One for standard DPIA.

5. Data Sharing

5.1 Who do we share your personal data with?

We sometimes share your personal data with trusted third parties.

When we share your data, we make sure that:

- We provide only the information they need to perform their specific services.
- They may only use your data for the exact purposes we specify in our contract with them.
- We work closely with them to ensure that your privacy is respected and protected at all times.
- If we stop using their services, any of your data held by them will either be deleted or anonymised.

5.2 Sharing your data with third parties for their own purposes:

We will only do this in very specific circumstances, for example:

- We may be required to disclose your personal data to the police or other enforcement, regulatory or Government body, upon a valid request to do so.
- For fraud management, we may share information about fraudulent or potentially fraudulent activity on our premises or in our systems. This may include sharing data about individuals with law enforcement bodies.

We currently share personal information with the following organisations who will process your data as part of their contracts with us:

- *NHS Halton CCG*
- *North West Boroughs Healthcare NHS Foundation Trust*
- *Royal Liverpool and Broadgreen University NHS Trust*
- *Aintree University Hospitals NHS Foundation trust*

6. Security measures

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 certified by the EU Privacy Shield and ISO 27001. Further information regarding how Google Analytics safeguards your data can be found here.

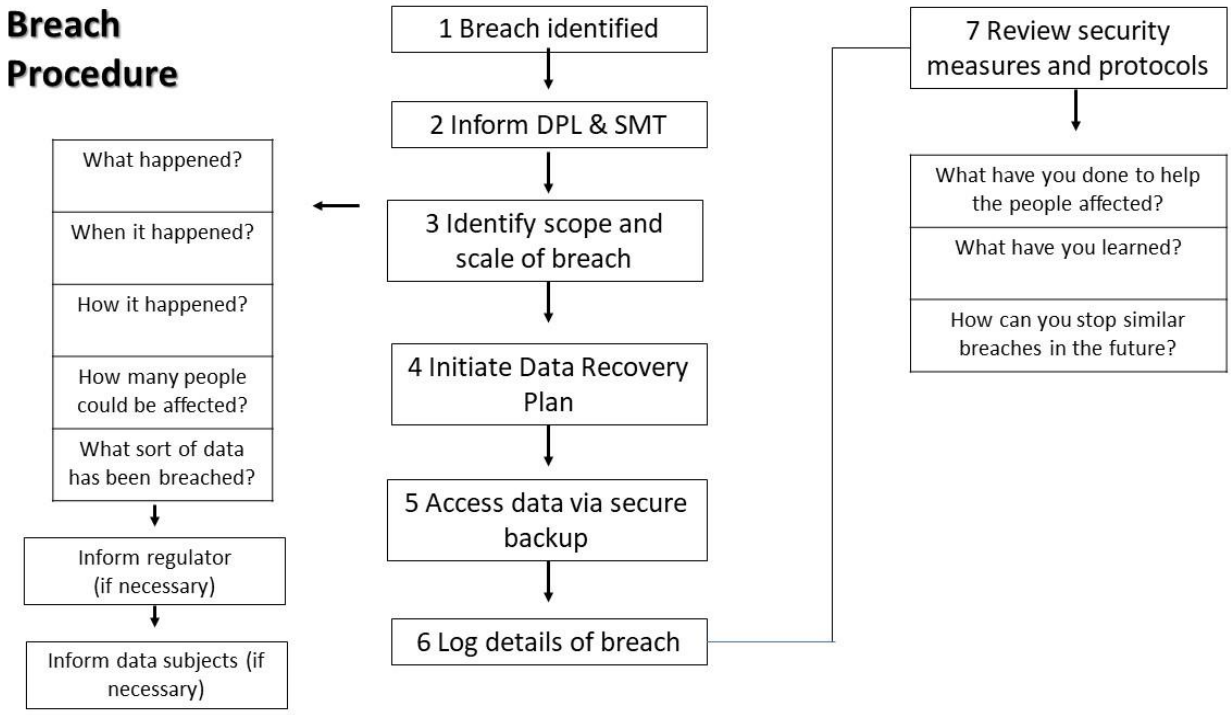
Access to your electronic personal data is password-protected and can only be accessed when on Wellbeing Enterprises office premises. Copies of paper based personal information is locked away securely in our filing systems and does not leave the premises

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

6.1 Breach procedure

If we become aware of any breaches to your data we will aim to inform you without undue delay. We will also inform the ICO of any confidentiality breaches within 72hrs of becoming aware of any such occurrence.

In the event of a data breach, the following procedure will be executed:

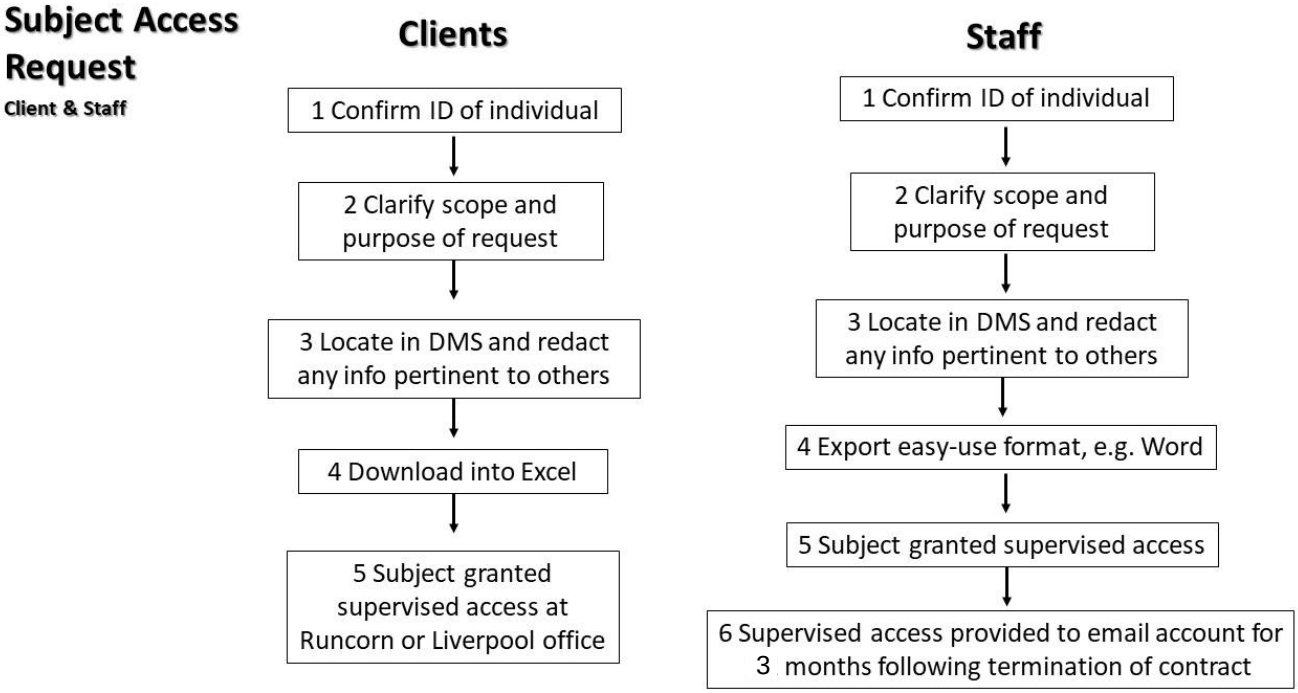


7. Subject Access Requests

All individuals who are the subject of data held by Wellbeing Enterprises are entitled to:

- Ask what information the organisation holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

7.1 Subject Access Request process

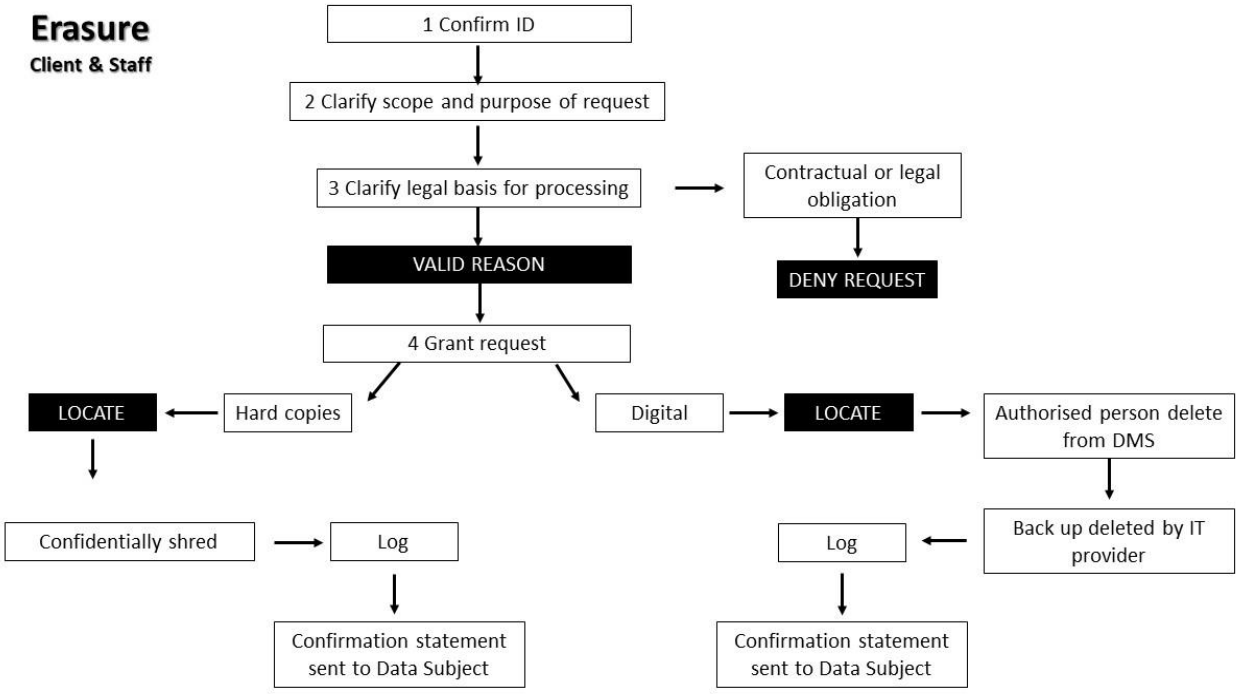


8. The Right to Erasure (Right to be Forgotten)

In certain circumstances, individuals have the right to have their personal data erased. You may exercise this right if:

- The personal data is no longer necessary for the purpose which we originally collected or processed it for.
- Consent was the original lawful basis for collection and you wish to withdraw your consent.
- Legitimate interests were the original basis for processing and you object to the processing of your data. If there is no overriding legitimate interest to continue processing your data then you may request for it to be erased.
- We are processing the personal data for direct marketing purposes and you object to that processing.
- We have processed your personal data unlawfully.
- We have to do it to comply with a legal obligation.
- We have processed the personal data to offer information society services to a child.

8.1 Erasure of Data process

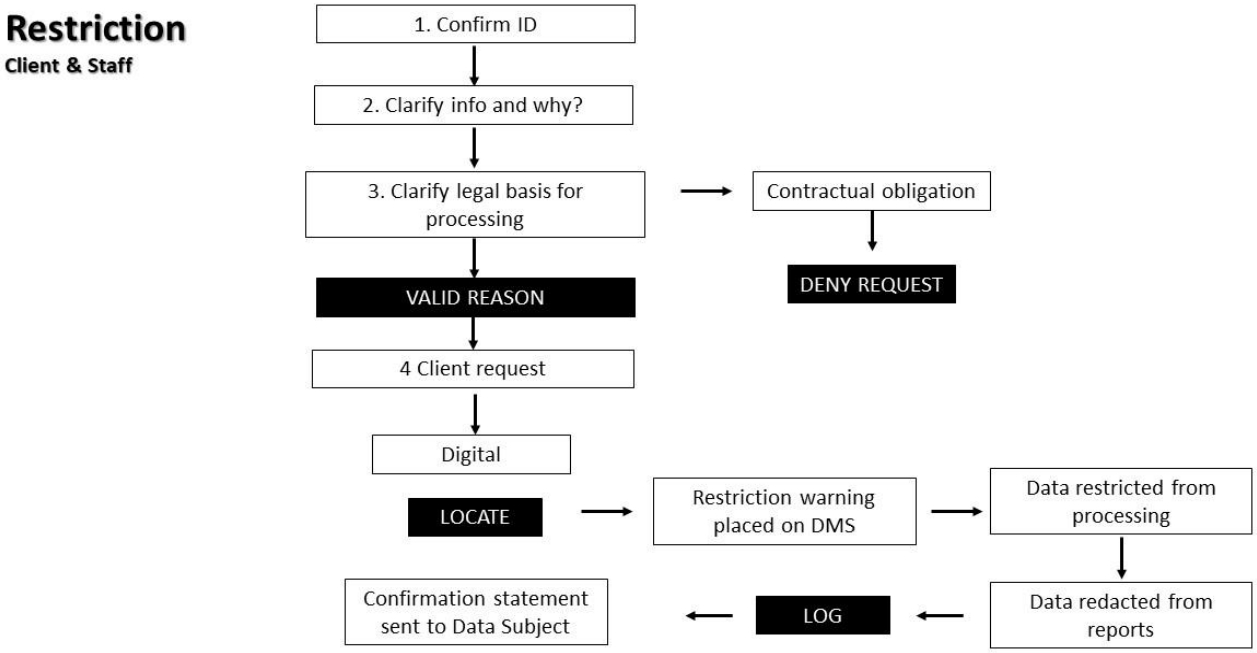


9. The Right to Restrict Processing

In certain circumstance, individuals have the right to request the restriction of their personal data. You may exercise this right if:

- You contest the accuracy of the personal information that is stored and we are in the process of verifying the accuracy of the data
- The data has been unlawfully processed and you oppose erasure – here you may request restriction instead
- We no longer need the personal data but you need us to keep it in order to establish, exercise or defend a legal claim
- You have objected to us processing your data and we are in the process of considering whether our legitimate grounds override your objection.

9.1 Data Restriction Process



10. 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/

11. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be 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. Regularly test the privacy measures implemented and maintain records of the testing and outcomes.

3. Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.

4. Keep records showing training of employees on privacy and data protection matters.

5. ICO registration renewed annually. Current registration number is: Z9945371

Contact Us

The primary point of contact for all issues arising from this privacy notice, is our Informal Data Protection Lead. The Informal Data Protection Lead can be contacted in the following ways:

Email: m.swift@wellbeingenterprises.org.uk
Telephone number: 01928 589799
Postal address: Bridgewater House, Old Coach Rd, Runcorn, WA7 1QT

If you have any questions, concerns or complaints regarding our compliance with this policy and the data protection laws, or if you wish to exercise your rights, we encourage you to first contact Wellbeing Enterprises CIC. We will investigate and attempt to resolve complaints and disputes and will make every reasonable effort to honour your wish to exercise your rights as quickly as possible and in any event, within the timescales provided by data protection laws.

11.1 To contact your data protection supervisory authority

You have a right to lodge a complaint with your local data protection supervisory authority (i.e. your place of habitual residence, place or work or place of alleged infringement) at any time. We ask that you please attempt to resolve any issues with us before your local supervisory authority.

12. The use of mobile phones and devices

12.1 Smart Phone Access Authorisation

For a member of staff to obtain a work issued phone their relevant Line Manager should ensure the user complete a mobile device assignment form.

The type of smart phone available for use will be decided by Mark Swift.

Before a phone is transferred from one staff to another a full factory reset should be completed.

Technical problems or queries regarding remote access or mobile devices should be addressed to ***Lynn Swift.***

12.2 Authorised Smart Phones

We maintain a log of all smart phones issued in our Information Asset Register.

All smart phones issued will be installed with appropriate PIN control.

Users must return all smart phones to Lynn Swift when access is no longer required, or when leaving the organisation.

12.3 User Responsibilities for the Security of Smart Phones

All smart phones should be held and transported securely, should not be left unattended (e.g. in vehicles), and should be locked away when not in use.

Stolen or lost equipment must be reported as soon as possible to Lynn Swift.

Users must not install any unauthorised or unlicensed software on any Wellbeing Enterprise issued smart phone

Issued smart phones should not be used for non-business-related purposes.

Issued smart phones must only be used by the individual that they have been issued to. A user may not share the device with or lend it to anyone else, for example a family member or work colleague.

12.4 User Responsibility for the Security of Personal Confidential Data and Information

Our data must not be remotely accessed, held and processed on smart phones supplied. There are safeguards in place to prevent access to organisation data in this way.

Users are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems. Smart phones should not be shared with any other person, even for temporary access to a non-work related app or service. Smart phone screens should be locked when not actively being used.

The use of smart phones in a public area should be kept to an absolute minimum, due to the risk of information being viewed and the theft of equipment.

Staff must ensure that Wellbeing Enterprises smart phones and information accessed at home are secure from theft and damage and cannot be accessed by family members, friends or any other unauthorised user.

Data should not be held on a smart phone for longer than it is required and should be deleted or archived promptly to reduce the risk of the data being accessed by the wrong person.
Personal confidential data must not be stored on issued smart phones.

Emails containing personal confidential data and other confidential information must not be sent to or from any email accounts.

12.5 User responsibility for the use of Personal Smart Phones

Users will not use personal smart phones to access our services or data.

User's will not store any Wellbeing Enterprises confidential data on personal smart phones

User will not attempt to connect to the organisation's corporate wireless network with personal smart phones.

12.6 Use of Public WIFI

Public WIFI and unsecured WIFI are not to be used whilst performing Wellbeing Enterprises duties. Public WIFI and unsecured WIFI are not secure.

Data must not be remotely accessed at any time.

When connecting to the internet use the phone's 3G/4G/5G connection.

13. Password Complexity Requirements

Users must follow the below password complexity requirements, when creating new passwords.

- be at least 8 characters long
- contain at least one lower case letter
- contain at least one upper case letter
- contain at least one number
- contain at least one symbol
- Not be reused

Passwords must be changed every 90 days.

Appendix One: Data Protection Impact Assessment

Wellbeing Enterprises CIC
Information Governance
Data Protection Impact Assessment (DPIA)

This assessment should be completed as part of the business case for all new information systems and processes which involve the use of personal sensitive data or will significantly change the way in which personal data is handled.

Once the assessment has been completed, please forward to the DPL/SMT for approval.

Project Name:	
Organisation:	
Department	
Name of individual completing DPIA screening:	
Designation of individual completing PIA screening:	
Telephone Number:	
Email:	

1. General Overview		
1.1	What is the name of the new system or process:	
1.2	Who is the responsible Lead for the new system or process (name & email address)?	
1.3	What are the main aims of the project?	
1.4	Provide the main activities of the project:	
1.5	What are the intended outcomes of the project?	
2. Information Asset Register		
2.1	Who is the Information Asset Owner (IAO) (Name & email address) – for <CoName> Staff only	
2.2	Who is the Information Asset Administrator (IAA) (name & email address if applicable) – for <CoName> Staff only	

3. Data		
3.1	Provide an indication of the Data Subjects (e.g. the living individuals whose data will be processed and held in the new system or process – include patients and/or staff)	
3.2	What classes of data will be processed and stored on this system or process (i.e. the data field descriptions)?	
3.3	Will the new or modified system or process include data which was not previously collected?	
3.4	What is the likelihood of loss of the data causing any unwarranted distress or damage to individuals concerned?	
3.5	Describe the legal basis for holding and processing this data?	
3.6	Does the system or process include new or amended identity authentication requirements that may be intrusive?	
3.7	Have checks been made regarding the adequacy, relevance and necessity of data used?	
3.8	Can the system or process use pseudonymisation and or anonymisation techniques?	
3.9	Is there an opt-out function whereby data subjects can request that their data is not used or stored by the new system or process.	
3.10	Has this been publicised?	
3.11	Who are the partners for the data sharing arrangement?	
4. Data Security		
4.1	Who will use the system or process and have access to the data?	
4.2	What training have users had in patient confidentiality?	

4.3	Will the data be shared with any other organisation(s)?	
4.4	What format will data be stored in?	
4.5	Where will data be stored?	
4.6	Does the system or process change the way data is stored?	
4.7	How will staff access and amend data	
4.8	How will data be shared? • Fax • Email • Via NHS Mail • Website • Via Courier • By hand • Via post – internal • Via post - external • Via telephone • Other – please state Please provide a data flow mapping of the data to be used in the system or process	
4.9	Are you transferring any personal and / or sensitive data to a country outside England, the UK or the European Economic Area (EEA)? If yes, please outline the data types, country, transfer methods and any measures in place to ensure adequate levels of security when transferred to this country.	
4.10	What security measures have been taken to protect the data?	
4.11	Is there a useable audit trail in place for the information asset(s)? For example, to identify who has accessed or amended a record	
4.12	How often will the system/process be audited and who will carry out the audit?	
4.13	Who supplies the system or process?	
4.14	Is the supplier of the system or process recipient of the data registered with the ICO? (please give registration number)	
4.15	Has the organisation completed the NHS Digital IG Toolkit to a satisfactory level? Include the IG Toolkit and organisation ODS code	

4.16	Does the contract between <CoName> and the supplier include necessary IG clauses?	
4.17	What business continuity plans are in place in the case of data loss / damage as a result of human error / computer virus / network failure / theft / fire / flood / other disaster?	
4.18	When was the business continuity plan last tested?	
5. Data Quality		
5.1	Who provides the information for the system or process?	
5.2	Who inputs the data into the system or process?	
5.3	Who will ensure that the information is kept up to date and checked for accuracy and completeness?	
5.4	Can an individual (or a court) request amendments or deletion of data from the system or process?	
6. Ongoing Use of Data		
6.1	Will the data be used to send direct marketing messages?	
6.2	If yes, are positive consent and opt-in procedures in place?	
6.3	Does the system or process change the medium for disclosure of publicly available information?	
6.4	Will the system or process make data more readily accessible than before?	
6.5	What is the data retention period for this data? (please refer to the Records Management Lifecycle)	
6.6	How will the data be destroyed when it is no longer required?	
7. DPIA Sign Off		

7.1 .	Your DPIA should be sent to the Information Governance Team for approval Approval by SIRO and Caldicott Guardian:	
	Date of DPIA Approval:	
	Name of IG Approver:	
	Title of IG Approver:	
8. Additional Actions		
8.1	Recommendations & required further actions following DPIA approval.	
8.2	Has the DPIA register been updated?	
8.3	Has the DPIA been presented to the IG Sub Group for comment / ratification?	

Appendix Two: Subject Access Request Form

Application for access to your personal data held by Wellbeing Enterprises CIC

Subject to certain exceptions, you have a right to have access to and / or correct any personal information that Wellbeing Enterprises holds about you (your 'personal data').

If you wish to make a Subject Access Request, please complete this form carefully and follow the instructions regarding the provision of proof of identity and details of how to return the form to Wellbeing Enterprises.

The purpose of this form is to ensure that all necessary information to complete your Subject Access Request is provided to Wellbeing Enterprises. You are not obliged to use this form, but if you do not, please ensure that all necessary information on this form is provided to Wellbeing Enterprises.

The term “data subject” refers to the person about whom the information is being requested

You can use this form to ask to see a copy of personal data that we hold about you, in line with data protection legislation.

You can also use this form to ask to see the records on behalf of someone else, as long as you are legally allowed to act on their behalf. This includes:

- Making a request for a child
- Making a request for someone that you have power of attorney for.

You should fill in all sections of the form that apply to you.

Please make sure you complete all relevant sections in block capitals to ensure that details are clear.

Section 2 should only be completed if you are making the request on behalf of someone else.

Section 1: Details of the person this request is about (the 'Subject')

Please tell us the details below about you, or the person you are applying on behalf of, so that we can check for the information we may hold:

Title	
Surname	
First Name	
Former Surname	
Date of Birth	
Gender	
Contact Number (day)	
Email Address	
Home Address (inc. postcode)	

Getting as much information as possible helps us find the information you want. If you/the subject has been known by a different name or has lived at a different address during the time span of your enquiry, please give details below:

Name:	**From (date):**	**To (date):**
Address (inc. postcode)		
Name:	**From (date):**	**To (date):**
Address (inc. postcode)		

Section 2: Written authority to act on behalf of the person you are making the request for

This section should only be completed if you are making the request on behalf of someone else.

If you are not the subject, but are acting on behalf of the subject, please tell us the details below. We need to know what gives you the authority to act on their behalf, so please state your relationship with them, for example, parent, solicitor, or holder of power of attorney.

Full Name	
Relationship with the subject	
Contact Number	
Email Address	
Address	

Section 3: Proof of Identity

Please do not send any original documents. You can send printed copies or electronic copies. (The following list is not exhaustive).

Applying for yourself
If you are applying for yourself, we need to see:

- one document confirming your name, from Group A, below
- one document confirming your address, from Group B, below

Applying on behalf of someone else
If you are applying on behalf of someone else, we need to see:

- one document confirming your name, from Group A, below
- one document confirming the name of the person you are applying on behalf of, from Group A, below
- one document confirming your address, from Group B, below
- one document confirming the address of the person you are applying on behalf of from Group B, below
- all documents needed to show that you have the authority to access the records, from Group C, below.

A. Documents that confirm your name:
- Full driving licence
- Passport
- Birth certificate
- Marriage or civil partnership certificate

B. Documents that confirm your address:
- Utility bill
- Bank statement
- Credit card statement
- Benefit book
- Pension book

C. Documents that confirm you are allowed to act on behalf of the person you are making the request for:
- Health and Welfare Lasting Power of Attorney
- Court of Protection Order appointing you as a personal deputy for the personal welfare of the Subject
- Full birth certificate of child
- Full certificate of adoption
- Parental responsibility order
- Signed declaration from the subject

We may get in touch with you for further information.

Section 4: Helping us to find the information

Please use the space below to provide details that may help to locate your information. Being clear about the information you require will help us to respond promptly to your request. If you think you require further information you can always submit a further request and there are no fees attached to your right of access. Please supply as much detail as possible.

Section 5: where you would like the copies of your information to be sent

Our preferred method of delivery is via email. Any documents sent will be password protected and sent securely.

If you would like to get your information by post, please note that information posted by special delivery will need a signature upon receipt. However, if the Royal Mail are unable to deliver to the address given and need to return the documentation to Wellbeing Enterprises this will be returned by normal post (that is, not securely).

Please tell us where you would like your information sent **(please select one option):**

☐ I am the Data Subject and would like my information sent to my email address given in Section 1.

☐ I am the Data Subject and would like my information posted to my home address given in Section 1.

☐ I am acting on behalf of the Data Subject and would like the information sent to the email address given in Section 2.

☐ I am acting on behalf of the Data Subject and would like the information posted to the address given in Section 2.

Section 7: Declaration

Unless there is Health and Welfare Lasting Power of Attorney or the application is being made on behalf of a child under the age of 13, everyone named on this form should sign below.

I confirm that the information that I have supplied in this application is correct, and I am the person to whom it relates, or I am acting on behalf of the Data Subject and have enclosed the relevant proof of authority as detailed in Section 3.

Your personal data will be kept in accordance with Data Protection procedures.

Data Subject:

Signature: ……
Date: ……

Print Name: ……

Person making a request on behalf of the data subject:

Signature: ……
Date: ……

Print Name: ……

Appendix Three: Erasure of Data Checklist

Before actioning any request for Erasure of Data, escalate to a member of the Senior Management Team to clarify legal basis for request and to make sure Wellbeing Enterprises do not breach any terms of contracts.

1. Confirm ID ☐
2. Clarify reason for request ☐
3. Clarify legal basis for processing (Escalate to SMT) ☐
4. If approved, grant request:
    a. Locate hard copy ☐
    b. Confidentially shred ☐
    c. Log ☐
    d. Locate digital file on DMS ☐
    e. Lynn Swift to delete from DMS ☐
    f. Contact DMS provider to delete information ☐
    g. Log ☐
    h. Confirm with person who raised request that this has been actioned ☐

Appendix Four: Data Restriction Checklist

Before actioning any request for restriction of data, escalate to a member of the Senior Management Team to clarify legal basis for request and to make sure Wellbeing Enterprises do not breach any terms of contracts.

1. Confirm ID ☐

2. Clarify reason for request – which information does the subject wants to be erased and why ☐

3. Clarify legal basis for processing (Escalate to SMT) ☐

4. If approved, grant request:
    a. Locate information on DMS ☐
    b. Place a restriction warning on subjects' file on DMS ☐
    c. Data to be restricted from processing ☐
    d. Data removed from all reports ☐
    e. Confirm with person who raised request that this has been actioned ☐