



# DATA PROTECTION POLICY

This Policy has been approved & authorised by:

**Name:** Mark Swift

**Position:** CEO

**Date:** 03/12/2025

**Signature:** 

This Policy has been approved & countersigned by:

**Name:** Tim Phillips

**Position:** Director

**Date:** 03/12/2025

**Signature:** 

Policy last reviewed on: 20/01/2026

Policy last reviewed by: MS

Policy next due for review: 20/01/2027

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

t: 01928 589799

e: [info@wellbeingenterprises.org.uk](mailto:info@wellbeingenterprises.org.uk)

## HUMAN RESOURCES POLICY TRACKING SHEET

Amendment	Reason for amendment	Date
<i>Policy Reviewed</i>	ICO ref updated page 15	23/10/2019
	<i>IDPO and Data Protection leads names removed from Policy and Mark Swift added (pg5,6 &amp; 15)</i>	08/11/19
<i>Policy Reviewed</i>	<i>List data shared with amended page 9; Happy Place App mentions removed, page 5, 6, 7 and 9; formatting pages 27 and 28</i>	10/02/2021
<i>Policy Amendment</i>	<i>Phone and device section 12 Password complexity section 13</i>	03/06/2021
<i>Policy Amendment</i>	<i>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.</i>	08/12/2021
<i>Policy Amendment</i>	<i>Rewritten to remove Privacy Notice material and focus directly on data protection issues</i>	22/12/2021
<i>Policy review</i>	<i>No Amendments</i>	25/01/2023
<i>Policy Review</i>	<i>No Amendments</i>	22/11/2023
<i>Policy Amendment</i>	<i>DPO updated to R Phillips pg 5</i>	11/04/2024
<i>Policy Review</i>	<i>1.3 updated to include Volunteers</i>	19/03/2025
<i>Policy Review</i>	<i>Full review and rewrite to include legal and framework updates and further clarification on roles and responsibilities.</i>	19/11/2025
<i>Policy Review</i>	<i>9.5 and 16. Updated training requirements to include full training every two years with annual refresher training.</i>	20/01/2026

# Data Protection Policy

1. POLICY STATEMENT	4
2. PURPOSE OF THE POLICY	4
3. SCOPE	4
4. DEFINITIONS	5
5. DATA PROTECTION PRINCIPLES	5
6. LAWFUL BASIS FOR PROCESSING	5
7. INDIVIDUAL RIGHTS	6
8. SUBJECT ACCESS REQUESTS (SARS)	6
9. ROLES AND RESPONSIBILITIES	6
9.1 Board of Directors	6
9.2 Chief Executive Officer (CEO)	7
9.3 Senior Management Team	7
9.4 Data Protection Officer (DPO)	7
9.5 All Staff and Volunteers	7
9.6 Data Processors	8
10. DATA SHARING AND THIRD PARTIES	8
11. INTERNATIONAL TRANSFERS	9
12. DATA RETENTION AND DELETION	9
13. DATA BREACHES	9
14. SECURITY MEASURES	10
15. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)	10
16. TRAINING AND AWARENESS	11
17. MONITORING AND ACCOUNTABILITY	11
18. RELATED POLICIES AND DOCUMENTS	11
19. REVIEW OF POLICY	12
APPENDIX ONE - PRIVACY BY DESIGN	12

## 1. Policy Statement

Wellbeing Enterprises CIC (WE) is committed to protecting the privacy, rights, and freedoms of all individuals whose personal data we collect and process. We handle personal data responsibly, lawfully, fairly, and transparently in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant national guidance issued by the Information Commissioner's Office (ICO). WE recognises that the people who use our services, our staff, volunteers, and partners trust us with important information. We take this responsibility seriously and maintain robust policies, procedures, and controls to safeguard personal data against loss, misuse, or unauthorised access.

This policy sets out how WE meets its legal obligations and ensures accountability in the processing of personal data.

## 2. Purpose of the Policy

The purpose of this policy is to:

- Ensure lawful, fair, and transparent processing of personal data
- Protect the rights of individuals
- Establish clear principles, responsibilities, and procedures for data protection
- Support compliance with UK GDPR and the Data Protection Act 2018
- Prevent data breaches and ensure prompt, responsible action when incidents occur
- Ensure staff, volunteers, and contractors understand their responsibilities

This policy forms part of WE's governance framework and must be followed by all individuals who handle personal data.

## 3. Scope

This policy applies to:

- All employees (permanent, temporary, or fixed-term)
- Volunteers
- Directors and Trustees
- Contractors, agency staff, and students
- Any third party processing data on behalf of WE (Data Processors)

This policy covers all personal data processed by WE, including:

- Electronic data
- Paper records
- Images, audio, and video recordings
- Data held on laptops, mobile devices, and removable media
- Data shared internally or externally

## 4. Definitions

- Personal Data: Any information relating to an identifiable person (e.g., name, contact details, NHS number).
- Special Category Data: Highly sensitive data such as health information, ethnicity, religion, and sexual orientation.
- Processing: Any operation performed on personal data, including collecting, storing, sharing, and deleting.
- Data Subject: The person whose data is being processed.
- Data Controller: WE determines the purposes and means of processing personal data.
- Data Processor: A third party processing data on WE's behalf.
- DPO: Data Protection Officer.
- DPIA: Data Protection Impact Assessment.
- Confidential destruction methods: secure disposal techniques such as cross-shredding, secure bin disposal, certified digital wiping, or professional confidential waste services.

## 5. Data Protection Principles

WE adheres to the seven principles of UK GDPR:

1. Lawfulness, Fairness, Transparency – Data is processed lawfully and individuals are informed.
2. Purpose Limitation – Data is collected for specific, explicit, legitimate purposes.
3. Data Minimisation – Only data necessary for the purpose is collected.
4. Accuracy – Data is kept accurate and up to date.
5. Storage Limitation – Data is retained only for as long as necessary.
6. Integrity and Confidentiality – Data is held securely.
7. Accountability – WE is responsible for demonstrating compliance with all these principles.

## 6. Lawful Basis for Processing

WE processes personal data under one or more lawful bases:

- Public Task – delivering services in the public interest
- Legitimate Interests – where processing is necessary for organisational function and does not override individuals' rights
- Consent – for specific, informed, freely given agreements
- Contract – when processing is necessary for employment or service provision
- Legal Obligation – compliance with law
- Vital Interests – to protect life in emergencies

Special Category Data is processed only when an additional condition applies, such as explicit consent or public health grounds.

## 7. Individual Rights

WE recognises all data subject rights under UK GDPR, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (where applicable)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights relating to automated decision-making

WE will respond to all rights requests lawfully, promptly, and transparently.

## 8. Subject Access Requests (SARs)

Individuals may request access to their personal data at any time.

WE will:

- Acknowledge SARs promptly
- Respond within one month, unless an extension is legally justified
- Verify identity before releasing information
- Redact third-party information where required
- Refuse or limit requests only in line with legal exemptions

Subject Access Requests should be submitted in writing to Kristina Tischendorf, Data Protection Officer. The DPO oversees the SAR process to ensure impartiality and compliance.

## 9. Roles and Responsibilities

### 9.1 Board of Directors

The Board of Directors has overall accountability for ensuring that Wellbeing Enterprises CIC complies with data protection law. Directors must provide strategic oversight, ensure adequate resources, and maintain appropriate governance.

Tim Phillips, Board Director, acts as the Executive Lead for Data Protection Compliance, with responsibility for championing robust practice and supporting monitoring, review, and continuous improvement.

## 9.2 Chief Executive Officer (CEO)

The Chief Executive Officer is responsible for ensuring that robust data protection practices are embedded across the organisation.

The CEO will:

- Keep the Senior Management Team and Board of Directors informed about data protection issues, risks, and responsibilities
- Ensure that Data Protection Impact Assessments (DPIAs) are completed for all new systems, services, or changes to processing
- Oversee the development and maintenance of data protection and security policies and training and ensure they are implemented consistently across the organisation
- Ensure that data processing agreements and contracts with third-party providers meet UK GDPR requirements
- Ensure that systems, services, and equipment used to store or process personal data meet accepted security standards and are regularly reviewed
- Ensure clear, accessible privacy notices are maintained and that individuals understand how their information is used and how they can exercise their rights

## 9.3 Senior Management Team

- Ensure organisational compliance with data protection law
- Approve policies and oversee risk management
- Support mandatory training for all staff

## 9.4 Data Protection Officer (DPO)

Kristina Tischendorf is the Data Protection Officer for Wellbeing Enterprises CIC. E: [k.tischendorf@wellbeingenterprises.org.uk](mailto:k.tischendorf@wellbeingenterprises.org.uk)

In accordance with UK GDPR, the DPO will:

- Inform and advise on data protection obligations
- Monitor compliance with policies, training, and audits
- Provide guidance on DPIAs and high-risk processing
- Serve as the primary contact point for the ICO
- Oversee breach investigation, risk assessment, and notification duties

The Executive Lead for Data Protection is: Mark Swift  
[m.swift@wellbeingenterprises.org.uk](mailto:m.swift@wellbeingenterprises.org.uk)

## 9.5 All Staff and Volunteers

All staff and volunteers share responsibility for protecting personal data and must:

- Complete mandatory data protection training / cyber security training, including anti-phishing, at induction, with annual refresher training and full re-certification every two years
- Follow all data protection and security policies
- Report any incidents, breaches, or concerns immediately
- Process personal data only when required for their role and only for authorised purposes
- Maintain confidentiality and security at all times
- Use strong, confidential passwords and never share them
- Ensure personal data is not disclosed to unauthorised individuals, internally or externally
- Avoid sharing personal data informally or through unsecured methods
- Store paper and digital records securely, following the Security Policy
- Regularly review the data they hold and ensure it is accurate, relevant, and up to date
- Delete or securely dispose of data that is no longer required, in line with the retention schedule
- Seek advice from their line manager or the DPO if unsure about any aspect of data protection

Failure to comply with this policy may result in disciplinary action.

## 9.6 Data Processors

- Must comply with Article 28 agreements
- Must follow WE instructions and security standards

Data processors must implement appropriate technical and organisational measures to meet the requirements of UK GDPR and ensure the protection of the rights of individuals.

Data processors must not subcontract processing without written authorisation from WE, and must notify WE immediately if they become aware of a data breach.

## 10. Data Sharing and Third Parties

WE may share personal data with:

- Health, care, and wellbeing partners
- Local authorities and statutory bodies
- Funders and commissioners (anonymised wherever possible)
- Data processors providing IT, analytics, or administrative support

For further detail on data sharing practices, see the WE Privacy Notice.

All sharing must:

- Have a lawful basis

- Be limited to what is necessary
- Be governed by appropriate contracts or agreements

WE does not sell personal data.

## 11. International Transfers

WE stores and processes data within the UK wherever possible.

If international transfers are required, WE will ensure appropriate safeguards such as:

- UK Addendum to EU Standard Contractual Clauses
- Adequacy regulations
- ICO-approved mechanisms

## 12. Data Retention and Deletion

WE follows a documented retention schedule. Key examples:

- Adult client records: 8 years after last contact
- Children's records: until age 25 (or 26 if seen at age 17)
- Employee records: 6 years after employment ends
- Recruitment records: 12 months
- Financial records: 7 years

All staff are responsible for ensuring that records are securely destroyed in line with this schedule. Data will be securely destroyed when no longer required, using appropriate confidential destruction methods.

## 13. Data Breaches

A data breach is any security incident leading to:

- Loss
- Unauthorised access
- Theft
- Alteration
- Disclosure of personal data

All breaches must be reported immediately to the DPO.

WE will:

- Investigate promptly
- Record breaches in the internal register
- Notify the ICO within 72 hours if risk is identified
- Inform affected individuals where there is high risk

- Take steps to contain and prevent recurrence

Failure to report a breach may lead to disciplinary action.

## 14. Security Measures

WE maintains strong technical and organisational measures, including:

- Encryption and secure servers
- Role-based access controls
- Multi-factor authentication
- Device management and endpoint protection
- Secure transfer protocols (SSL/TLS)
- Regular auditing and penetration testing
- Physical building security
- Business continuity and disaster recovery plans

Employees must follow the Security Policy at all times.

Further detail is provided in the WE Security Policy.

## 15. Data Protection Impact Assessments (DPIAs)

Privacy by Design is a core principle of the UK GDPR and is strongly promoted by the Information Commissioner's Office (ICO). Wellbeing Enterprises CIC is committed to ensuring that all new systems, services, and processes are developed and implemented in line with recognised Privacy by Design and Privacy by Default best practice (see Appendix One).

WE completes DPIAs where processing is high risk, such as:

- New systems or technology
- Processing Special Category Data
- Large-scale or sensitive monitoring
- Data sharing with new partners

DPIAs consider legality, necessity, proportionality, risks, and mitigating measures.

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 compliance

## 16. Training and Awareness

All staff and volunteers must:

- Complete mandatory data protection / cyber security training, including anti-phishing awareness, at induction
- Complete annual refresher training in data protection / cyber security
- Complete full data protection / cyber security training, including anti-phishing awareness, re-certification every two years
- Follow Wellbeing Enterprises CIC policies and procedures
- Understand how to recognise, respond to, and report data protection incidents and data breaches

Managers are responsible for ensuring that staff and volunteers comply with these requirements.

## 17. Monitoring and Accountability

Wellbeing Enterprises CIC recognises that data protection compliance is an ongoing responsibility. To ensure continuous compliance with the UK GDPR and the Data Protection Act 2018, WE will:

- Maintain documentation and evidence of all privacy measures implemented
- Keep an up-to-date Record of Processing Activities (ROPA)
- Review and update Data Protection Impact Assessments (DPIAs) regularly to ensure they reflect current practice
- Test and audit privacy and security measures, and record the outcomes
- Use audit findings, testing, and metrics to demonstrate continuous improvement
- Maintain an internal data breach log and monitor trends
- Keep records of staff training in data protection and information security
- Ensure ICO registration is maintained and renewed annually (Registration: Z9945371)

The Data Protection Officer monitors compliance and reports risks or concerns to the Senior Management Team and the Board of Directors.

## 18. Related Policies and Documents

- Security Policy
- Privacy Notice
- Confidentiality Policy
- Safeguarding Policies

## 19. Review of Policy

This policy will be reviewed every 12 months by the DPO and Senior Management Team and approved by the CEO and Board of Directors.

### Appendix One - 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.

