Confidentiality & Privacy Policy

Doc No: POL-QA-04

Policy Lead: Chief Executive Officer

Issue No:	Rev No:	Issue Date	Date of Board Approval	Review Date
1	5	May 2023	29 April 2023	April 2024

1. Introduction

This Policy should be read in conjunction with our Data Protection Procedure (PRO-QA-09), Data Protection Policy (POL-QA-09), Data Breach Procedure (PRO-QA-08) and with our Easy Read and Standard Read Privacy Guides.

The Chief Executive Officer, who is the Organisation's Data Protection Officer, has responsibility for overseeing implementation of this Policy.

2. Policy Commitment

We want everyone who comes in to contact with our service to feel confident and comfortable with how personal information you share with us will be looked after or used by Journey Enterprises.

This Confidentiality & Privacy Policy sets out how we collect, use and store your personal information. This means any information that identifies or could identify you. We also set out our commitments to ensure confidentiality whilst you are in contact with our service.

We are committed to treating you with respect and openness, ensuring your personal information is processed fairly and handled confidentially.

3. Registration and data control

Journey Enterprises is registered with the Information Commissioners Office (ICO) for the purposes of the Data Protection Act 1998 and (from 25 May 2018) the EU General Data Protection Regulation 2016/679 ("Data Protection Law"). This means that we are responsible for, and control the processing of, personal information.

This information relates to:

- current, past and prospective employees
- current, past and prospective volunteers
- current past and prospective trustees/directors
- Clients
- parents/carers
- professionals and organisations with whom we work
- suppliers
- regulators
- funders
- individual donors

Journey Enterprises has a Data Protection Officer who is the Chief Executive Officer. He/she is responsible for ensuring your data is handled in line with the requirements of the Data Protection Act (2018) and General Data Protection Regulation (2018).

If you would like further information about our privacy practices, please contact:

Elspeth McPherson
Chief Executive Officer
Journey Enterprises Ltd
Network House
Acomb
Northumberland NE46 4SA

Email: elspeth.mcpherson@journeyenterprises.co.uk
T: 01434 724039 (direct line)

4. How we collect personal information

Everything we do, we do to ensure that we can help people with learning disabilities to lead happy, fulfilling and socially-inclusive lives.

We collect information about people in the following ways:

When someone has direct contact with us

This could be an enquiry about our services, registering with us for our services, registering to attend an event, becoming a Member of Journey Enterprises, making a donation to us, applying to work with us (employment or volunteering), applying to become a Trustee or linking to us professionally as someone working for another organisation.

This may be by emailing us, telephoning or writing to us, or completing an online enquiry. When people visit our website www.journeyenterprises.co.uk we gather general information which might include which pages are visited most often and which services, events or information is of most interest to visitors.

5. The type of Information we collect

We collect personal information such as:

- your name
- date of birth
- email address
- postal address
- telephone number

For Clients in our service we will also collect information on:

- a photograph
- disabilities
- health conditions
- medication
- gender and sexual orientation
- faith and cultural identity

- the names of parents & carers
- the names of social workers, Care Managers & specialist nurses
- the name/address of the Client's GP/Surgery
- Social Services number if Clients wish to provide this
- National Insurance and NHS numbers if Clients with to provide these

For unpaid carers of dependents' in our service we may also hold information on:

- disabilities
- health conditions
- gender
- marital status
- employment status

For employees we will also hold information which includes:

- a photograph
- information on disabilities for those with reasonable adjustment needs
- information on illness (sickness absences)
- emergency contacts
- banking information (for payroll, pension and expenses)
- former names and addresses (for DBS & Right to Work checks)
- criminal records check/DBS
- two named professional referees
- evidence of qualifications & licensing
- National Insurance number (for administration of payroll and SMP/SSP)
- National Health number (for medical emergency use if employees wish this recorded on our Breathe HR platform)
- Evidence of 'right to live and work' in the UK (i.e. for non UK nationals)

For volunteers including trustees we will also hold information which includes:

- a photograph
- emergency contacts
- former names and addresses (for DBS & Right to Work checks)
- criminal records check/DBS
- two named professional referees

For regular donors we will hold information which includes:

- banking details (account number, sort code and name)

For Anti Money Laundering purposes, we also hold the following information on Designated Trustees, the Chief Executive Officer, Operations Manager, Business Support Manager and our contracted financial administration service (Counting House North East)

- years spent at current residential address
- former residential addresses if under three years at current address
- identity check evidence i.e. passport, photographic driving licence
- address evidence i.e. financial statement, utility bill et al

6. Sensitive Personal Information

Data Protection Law recognises that some categories of personal information are more sensitive. Sensitive Personal Information can include information about a person's health, race, ethnic origin, political opinions, sex life, sexual orientation or religious beliefs. Journey holds both anonymised records, collected during recruitment and surveys as part of our commitment to Equality & Diversity, and named records.

We hold named Sensitive Personal Information in relation to our Clients, unpaid carers and employees (where disclosed only in relation to reasonable adjustment needs). We treat this information with care and confidentiality and always in accordance with this Confidentiality & Privacy Policy.

- We will only use this information for the purposes for which we told you we were collecting the information.

- Access to this information will be restricted to those who need to know this information as part of their role.

- We will not pass on your details to anyone else without your express permission except in exceptional circumstances. Examples of this might include Safeguarding (risk to person) or in emergencies (health crisis or where a crime is being committed).

- We will only hold your data for as long as is necessary for us to deliver our services and to comply with regulators' requirements and UK law.

7. Fundraising & Marketing

As a small regional charity, Journey Enterprises does not undertake unsolicited fundraising or marketing activities. We will only contact you about our work and how you can support Journey Enterprises if you have agreed for us to contact you to discuss this. We will only use a contact method you have agreed e.g. post, email, telephone, text. You may withdraw this consent, or change your preferred contact method, at any time.

Journey Enterprises is committed to the Code of Fundraising Practice. We will not contact you after we have received a one-off donation to request an ongoing commitment, a conversion. We will not contact you after you set up a regular donation to request a higher donation amount.

8. Keeping your information safe on and off site

8.1 Journey Enterprises takes handling and use of personal information very seriously. We have appropriate physical, technical and organisational measures to protect the personal information we hold to keep data safe from improper access, use, alteration, destruction and loss.

8.2 All Staff (employees and volunteers) are required to work within our policies and procedures, respecting the sensitivity of personal data they may handle and the need for confidentiality when handling personal data.

8.3 Journey delivers services both from its operating sites and within the extended community requiring Staff to handle both personal and sensitive personal data with additional controls in place:

- Hard copies of personal data such as Client or Staff Files may only be taken from our premises if removal from the site is pre-approved by a Senior Manager and appropriate security measures are in place for the duration of the agreed period of withdrawal from our site;

- Hard copies of personal data, and mobile devices issued by Journey, may not be left unattended at any stage, for example, in staff cars, on public transport, in staff homes or in off-site venues;

- Hard and electronic copies of personal data should not be viewable by anyone un-authorized to access the data whether working on or off site;

- Staff working in community settings must also ensure that discussion of personal data should not be audible to anyone unauthorized to access the data. This includes face-to-face discussions and telephone-based discussions;

- Where meeting Clients, Staff or professionals off-site, venues should be pre-booked which enable appropriate levels of confidentiality;

- Personal data held electronically on Journey's mobile devices is encrypted with DESlock and is password protected. Personal data should not be sent electronically without a Senior Manager's consent for release and appropriate data encryption;

- In all cases where personal data has been agreed for release externally, the recipient must acknowledge receipt: for items posted Staff must use registered or recorded delivery; for items sent electronically, Staff must request a delivery and read receipt

8.4 Breaches of data protection are taken seriously: the actions we will take in the event of a data breach are set out in our Data Breach Procedure (PRO-QA-08). Where Staff are responsible for data breach breaches appropriate disciplinary, and corrective, actions will be taken without delay. In the case of serious procedural breach and loss or sharing of personal data, Staff may be suspended whilst a gross misconduct investigation is conducted.

9. How long we hold your information for

We only keep information for as long as it is reasonable and necessary. The length of time during which we hold different types of information is set out in our General Data Protection Regulation Record Retention Procedure (PRO-QA-06).

10. Your rights

10.1 Subject Access Requests

You have the right to request access to a copy of the personal information that we hold about you, along with information on what personal information we use, why we use it, who we share it with, how long we keep it for and whether it has been used for any automated decision making.

You can make a request for access free of charge by completing our Subject Access Request Form and providing evidence of your identity.

We will provide your data as quickly as possible.

Copies of our Subject Access Form can be obtained by contacting an administrator at your nearest Journey Hub:

Business Administrators

(Acomb Hub) helen.wood@journeyenterprises.co.uk
T: 01434 605185

(Coundon Hub) rachel.teasdale@journeyenterprises.co.uk
T: 01388 612 160

(Newcastle Hub) info@journeyenterprises.co.uk
T: 0191 484 1292

Completed requests and evidence of identity should be sent using secure/trackable mail to:

Elspeth McPherson
Chief Executive/Data Controller
Journey Enterprises Ltd
Network House
Acomb
Northumberland NE46 4SA

Please mark your envelope *'Private and Confidential'*.

10.2 Objections, Amendments, Restrictions and Removal of Data

You can object to our processing of your personal information and ask for it to be amended, restricted or removed.

Withdrawing Consent: if you have given us your consent to use personal information (for example, for providing a service to you or a member of your family), you can withdraw your consent at any time.

Rectification: You can ask us to change or complete any inaccurate or incomplete personal information held about you.

Erasure: You can ask us to delete your personal information where it is no longer necessary for us to use it, you have withdrawn consent, or where we have no lawful basis for keeping it.

Restriction: You can ask us to restrict the personal information we use about you where you have asked for it to be erased or where you have objected to our use of it.

In all cases please contact the Chief Executive/Data Protection Officer in writing, providing as much information as possible about the changes you want made. Please be aware that if we are legally required to keep information by law, for a funder or regulator, we may not be able to remove, change or restrict your information until this requirement has ended. We will inform you if this is the case and explain when we are able to make the changes you require.

12. Disclosure of Personal Information

Strict conditions apply to the disclosure of personal information both internally and externally. We will not disclose personal information to any third party unless we believe it is lawful to do so.

Where someone is at immediate risk, for example, is at risk of harm, self-harm or abuse, or if a crime is being committed, we may share personal data with relevant statutory bodies without consent. A Senior Manager's approval is required in all cases where consent has not been given. Where possible, no referrals should be made without the subject's consent to share their data.