Privacy Notice

Solo Support Services – Applications & Interview

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

Solo Support Services Ltd are committed to protecting your personal data. This privacy note explains:

- From where we secured your personal data;
- The personal data that we collect;
- Your personal data rights;
- Your right to object to our processing your personal data and withdrawing consent;
- How and when we use that personal data;
- Whether we share your personal data with anyone else;
- For how long will we keep your personal data;
- How you can access your personal data

If you have any questions or queries about this notice, please email us by clicking 'here'.

We have a Recruitment, Selection and Application Policy for employees to follow to ensure that we collect information in line with our legal and CQC registration obligations and that this is managed in line with UK-GDPR regulations.

Data Protection Officer
Our Data Protection Officer is Helen Brown, who is a member of the Senior Management Team, reporting to Director level. They have responsibility for monitoring GDPR compliance, supporting colleagues with enquiries and advice, conducting Data Protection Impact Assessments, liaising with external organisations such as the ICO, the management of data requests and data breach management.

Information Commissioner's Office Registration
We are registered with the Information Commissioner's Office (ICO), registration number Z2857587. A copy of our current certificate can be provided upon request.

Personal data that we collect:

Application Stage:
We always ensure that we have a lawful basis for processing the personal data that we collect. The justification for the personal data that we collect falls into different categories.

The justification for the processing of the following data is a 'Legitimate Business Interest', due to our responsibility to ensure our employees meet 'the Fit and Proper Person Requirement' under our CQC registration:

Name, address, email address, telephone number, education history, employment history, right to work documentation, UK visa information and criminal record history.

We collect your personal data from you at application stage. We do not collect personal data from third parties at initial application stage.

We recruit employees for care and support positions in conjunction with our clients. All personal data provided in your application is anonymised before sending to the client prior to an interview.

Interview Stage:

Should you be invited to attend an interview for one of our vacancies, we would need to collect the following personal data, the justification for the processing of this data is 'Legitimate Business Interest' due to our responsibility to check the identity of potential employees to ensure they meet both 'the fit and Proper Person Requirement' under our CQC registration and to ensure we meet employment law standards as defined by UK law.

Passport and / or driving licence.
Proof of National Insurance
Proof of Address

We collect your personal data from you at interview stage.

Your rights in respect of your personal data

You have the right to request access to your personal data, amendments to it and for it to be deleted.

Further information about those rights along with your right to withdraw any consent you've given or object to our processing your data can be found in our data protection policy, available within the employee handbook or by clicking 'here'. That policy also includes who to speak with if you have any queries about our approach to processing your personal data.

Where we store your data

Your personal data is stored on secure, password protected, cloud-based systems within the UK, EU and North America. We use the following systems: The Access Group (Care Planning and People Planner), BrightPay, Nest Workplace Pensions and also Google Drive for Business.

We use accepted standards of technology and security to protect your personal data and have collected confirmation from all suppliers that they adhere to UK GDPR legislation. Data is

encrypted for protection on each and all are password protected systems. Two step authentication is in place for Google Drive, device specific security is in place for Access.

Data is also stored within lockable physical personnel files within head office.

Who has access to your data?
Access to personal information is provided to Head Office based personnel who require this information to enable them to complete their role.

How and when we use your personal data
We're committed to using your personal data responsibly and lawfully. We only use your data to fulfil our duties as your employer, for example to provide you with updates regarding your employment or benefits, to process your payroll including tax, National Insurance via HMRC and to complete relevant employment checks.

To help us to maintain the accuracy of the personal data that we hold please let us know if we hold out of date or inaccurate information about you.

Sharing your personal data:
There are times where we will share your personal data with a third party. They are:

- With the Disclosure and Barring Service to obtain an enhanced DBS check, required for all employees under our CQC registration.
- With the Care Quality Commission (CQC) as part of our legal regulatory requirements.
- With BrightPay, our payroll provider, to allow us to process your payroll through a HMRC recognised system.
- With Access Care Planning, our Client Management System, a password protected site.
- With Google Drive for Business, where we store all our electronic files.
- With NEST or People's Pension, where you meet the eligibility criteria, under our obligation to provide a workplace pension.
- With our insurers, when required to report an incident or claim.
- When required by law.

We will request consent from you to process your information unless required by law.

How long we will keep your personal data.
Our 'Justifiable Retention policy' lists the type of data we process and for how long it is kept. You can access that policy by clicking 'here'. If you would like us to delete your data and we don't have a lawful reason to retain it you can make a deletion request by clicking 'here' or writing to Helen Brown, Data Protection Officer, 20 Central Avenue, West Bridgford NG2 5GR.

How you can access your personal data

You can ask us for a copy of the personal data that we hold on you by either clicking 'here' or writing to Helen Brown on the above address. We'll ask you for copies of two types of approved identity to process your request (such as a passport and driving licence). You can also ask us to

make corrections to data you consider to be inaccurate by clicking 'here' or again writing to Helen Brown.