Privacy Notice – Employment

This document sets out what information Springhill House (Accrington) Limited t/a Springhill Care Home collects from employees, how it uses the information, how it protects the information and your rights.

Springhill House (Accrington) Limited t/a Springhill Care Home is committed to ensuring your privacy is protected in accordance with Data Protection Standards.

Springhill House (Accrington) Limited t/a Springhill Care Home is using the following definition for personal Data:

Personal data	*Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.* *Personal data we gather may include: individuals' contact details, educational background, financial/credit worthiness and pay details, details of certificates and diplomas, education and skills, job title, and CV.*
Sensitive personal data	*Personal data about an individual's marital status, nationality, racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data will only ever be carried out with the express permission of the individual.*

Springhill House (Accrington) Limited t/a Springhill Care Home may change this policy from time to time by updating this page. This policy is effective from 1st May 2018 but we ask you to check this page from time to time. Any updates or changes to the use of your personal data will be advised to you, prior to that change of use.

What this Privacy Notices relates to.

This privacy notice relates to our employment processes

Who We Are?

Springhill House (Accrington) limited whose registered office is at 11 Cannon Street, Accrington, Lancashire, BB5 1NJ, United Kingdom

Contact Us

On-Line: https://www.springhillcare.com

Email: info@springhillcare.com

Phone: 01254 304500

Post: Springhill House (Accrington) Limited, 11 Cannon Street, Accrington, Lancashire, BB5 1NJ, United Kingdom

Our General Privacy Policy

This Privacy Policy relates to the specific activity identified above, however our general Privacy Policy is available on the privacy policies page of our website.

Your Rights

A copy of 'your rights' is available on the privacy policies page of our website.

What Personal Data are we collecting?

During the course of your employment with us, we will be processing the following information:

- Your full name, address and contact details, next of kin.
- Identification and legal status to work in the UK.
- References, qualifications and certifications including NMC PIN numbers that you have provided us with.
- Any specific health issues that you may be required to disclose depending on the nature of the role.
- Any other information that you provide in your CV or written application – that we have no control over.
- PAYE information and national insurance number.
- Your bank details, as we operate a BACS payment process and require this in order to be able to pay you.
- If your role involves travel, we may also need to obtain copies of your driving licence, car business insurance and/or passport in order for us to be able to arrange travel or hire cars.
- If your role entitles you to private medical or other health insurance, we may at some point be in possession of some of your medical data.
- Sickness reporting – if you report absence from work, there is the possibility that we may be consequently be in possession of information relating to your health, or potentially in possession of fitness to work assessments.

Are we likely to need any Sensitive Personal Data?

Yes. In some cases, you will be required to provide evidence that, depending on any medical condition you disclose to us, you are able to undertake the role we may offer you.

In some cases, we will also ask about communicable diseases or other conditions that may put you, other members of staff or our clients at any risk. We will only ask for this information if it is necessary and you will be made aware of this in the role profile.

In the event you voluntarily disclose information about your health, such as if you were to be absent from work due to sickness and/or in the event that we ask you to attend a medical to establish your fitness to work, we would consequently be in the position of processing sensitive health data.

We require you to provide us with any convictions, cautions, reprimands, warnings or pending prosecutions that you incur during your employment with us.

Why we need this information?

We need this information in order to:

1. Fulfil our contract with you – providing you the payment and benefits outlined in your contract / offer of employment.

2. To comply with the law or sector requirements to ensure the people in our care are safeguarded.

3. To fulfil and meet the requirements of the organisation and its objectives.

4. So that we can ensure that you are fit, well and able to fulfil your role and that we are aware of any issue that may affect you, other staff, our clients or the organisation.

What is the legal basis of processing?

We will only ask for information relevant to the role within which you are working, or progress on to undertake, subsequent processing will only be carried out where it is appropriate or where we are legally obliged to as part of our industry compliance requirements, where we are providing you a benefit by way of your contract or where we need to protect the interests of the company. You will be informed of any processing or sharing of data before it is shared.

The legal basis of processing your Personal Information is explained below:

Legal Basis	Explanation	Examples
Contractual Obligation	Where we have contracted with you to provide you a service or benefit as a result of your employment	Paying your salary into your bank account requires us to process your bank information.
		Providing your health, pension or other benefit may require us passing your details to a third-party provider – you will be notified before we do this

Legal Basis	Explanation	Examples
Legitimate Interest	Where we believe our legitimate interests do not override your interests, rights and freedoms	Requesting you to attend a medical after a period of sickness and obtaining confirmation of your fitness to work or medical conditions that may limit your duties.
		We may be required to undertake screening e.g. display screen assessments, moving and handling assessments. We may record this information to provide evidence in the future for example if you were to make a claim.
Legal Basis	**Explanation**	**Examples**
Legal Obligation	This is where the organisation has a legal obligation to comply with current law, industry compliance requirements, court order etc.	Providing HM Revenue and Customs information about your employment, tax, national insurance contributions etc.
		Providing information to the company's legal team concerning employee's sensitive data and allegations in respect of employee relations cases.
		Compliance with a court order, earnings order, legal case, statutory duty with CQC and local authorities (safeguarding).

Legal Basis	Explanation	Examples
Legal Obligation		Providing anonymous statistical information for gender and equality compliance
		Where we are required to be able to demonstrate, mental and physical fitness to undertake role, skills and competences of our staff in order to comply with industry or legal requirements
		Collating information required to conduct a DBS check or to check the barred list.
Legal Basis	**Explanation**	**Examples**
Vital Interest	Where the collection or sharing of information is in the vital interest of you or other members of the public, including staff or clients.	Obtaining your next of kin details.
		Sharing appropriate identity information with a medical provider (Ambulance, doctor, hospital etc.) in the event you are taken ill, OR where the third-party may need to know this to obtain medical care for you in the event you are taken ill e.g. if you were taken ill whilst on a business trip.
		Where your condition may represent a threat to the interests, rights and freedoms of other people e.g. if you had a communicable disease and were required to work with vulnerable people

How do I withdraw consent or change my preferences?

You can object to us processing your data at any time by:

1. Informing the Human Resource team
2. By contacting us letting us know what you would like to change

Be aware that in some cases objecting to the processing or sharing of your information may result in a benefit being withdrawn or us being unable to comply with the law or our contract with you. You will be informed of how we can or cannot comply with your request, when/if you were to make such a request.

Some requests may also require a re-issue of your employment contract.

Some examples are:

"Please do not share my details with HMRC"	We would not be able to comply with this request as we are legally obliged to provide this information.
"I do not want to provide my bank details to you"	In this instance we would be unable to pay your salary. This would mean that we were unable to fulfil our contract with you and as such would be tantamount to a resignation by you.

What decisions are going to be made using my Personal Data?

Each role within the organisation is clearly defined by way of skill, experience, qualification requirements etc. Additionally, some roles also have specific requirements in relation to fitness and health status depending on the nature of the role. Roles involving the care or monitoring of vulnerable adults or children will also require criminal records checks, which we are required to do under law as part of our duty of care towards them.

In some cases, ongoing training, certification, re-certification and continuous personal development are either part of the role, your development plan or form part of the requirements for our organisation to comply with general law, industry law, or certifications. In these instances, it may be necessary for us to keep track of where employees are at with their own activities.

Is there any automated decision-making being applied to my Personal Data?

There is no automated decision-making being made using your Personal Data.

Will my information be shared with any third-parties?

We may share your data with the following third-parties:

1. Immigration Services to ensure that you have the right to work in the UK and/or correct visa requirements – this is based on our requirement to comply with the law surrounding recruitment.

2. Police and Criminal Records Bureau E.g. Disclosure and Baring Service check.

3. Certification bodies (Exam Boards, University, College) – as listed in your qualifications, we may be required to undertake this in compliance with our legal obligations and in any case in relation to our legitimate interests.

4. References – as provided by you based on our legitimate interest.

5. Medical Examiner – where we may require you to undertake a medical, hearing test, etc. or where your condition may require us to obtain independent medical advice relative to the role you have applied for. This may be both based on our legitimate interest but also, depending on the role, to protect you and/or other members of staff or our clients.

6. Industry Compliance / Audit – where we are required to comply with industry requirements e.g. register staff, demonstrate competences or accreditations, auditors etc. we may need to share only data that is limited to fulfilling that purpose necessary to demonstrate compliance. This may therefore fall under the category of legitimate interest or legal obligation, depending on the nature of the audit/compliance requirement.

7. Payroll – our management company Springboard Business Support Limited processes our payroll. We have undertaken checks to ensure that they comply, as a minimum, with the same level of security of processing around Personal Data as we do. Only the limited information necessary for them to undertake payment processing is shared with them. We are processing this information in order comply with our contractual obligations with you.

8. Government Services – HMRC, Pensions & National Insurance, Immigration, Courts, and Police – as required by law, order including attachment of earnings.

9. Nursing and Midwifery Council – where we are required to report a case if we believe the conduct, competence, health or character of a nurse or midwife presents a risk to resident's safety.

10. We are required to report to the DBS of any event that an employee is found to put our residents at risk of harm or caused harm. We are also required to disclose this information to the Care Quality Commission and the Local Authority as part of our statutory duty.

We use several consistent third-parties who act as Data Processors on our behalf to provide us specific services. We may share your data with them to enable us to undertake the activities as set out above. They themselves may then become Data Controllers once your data is shared with them.

These providers are set out below:

Company Name	Activity Undertaken	Personal Data Shared
Superpay	Outsourced payroll services	ID information, payroll, tax, pension, sickness pay, maternity pay, expenses and any data relating to your pay
NOW: Pensions	Pension Services	ID Information, payroll, tax and pension information
SAGE	Medical / Occupational Health	ID information, sickness records, relevant medical details
UCheck	Criminal Records Checks	ID Information
Trainline and hotel websites such as booking.com	Company Travel, bookings and hire	ID Information, Passport, Driving Licence
Employer legal helpline provided by FSB or our insurance provider	To seek advice in relation to employment relations	Name, DoB, performance, attendance, health and well-being.
NMDS, other training providers as required.	Training Platform	ID Information, qualifications and training records

All the companies above either comply with our privacy policy or have appropriate security measures in place in order that they comply with the requirements under data protection and GDPR legislation.

What safeguards are in place to protect my Personal Data?

Springhill House (Accrington) Limited operates a Security By Design and By Default methodology that means we are continually checking the security, both new and current. This enables us to adhere to the Privacy by Default and By Design principles.

We will not change the use of your Personal Data in respect of this policy or share your data with a third party (other than those outlined above), without informing you or obtaining your consent where possible unless it is for our legitimate interest and your interests, rights and freedoms are not affected.

Retention Period

Please see our Retention Policy for details of our retention periods, but in relation to employee's information is stored, overall, for as long as you are an employee, then for 8 years after you have left employment.

If you do not wish us to retain your data, then you have the right to be forgotten and we will at your request destroy your data where we can legally do so and/or where we do not have a legitimate interest to retain such information e.g. such as your hearing test results.

If your data is required for statistical analysis, then your Personal Data will be anonymised to ensure that it is no longer personally identifiable.

Security

Springhill House (Accrington) Limited operates a Privacy By Design and By Default policy. This means that before we use your data we have already considered the potential impact on you, were your data to be lost, stolen, shared or compromised.

We undertake routine reviews of our processes and security policies to ensure that we can take all reasonable precautions in protecting your data.

Where at all possible we encrypt all information that is either stored or transmitted to third-parties. Where data is stored or transmitted to a Third Country (any country outside of the European Economic Area (EEA)) we will ensure appropriate adequate protection is in place in accordance with Data Protection Legislation.

Consequently, we may also need to sometimes undertake further security and screening questions when undertaking our routine dealings with you. These are there to protect your personal data and security.

Whilst we undertake all reasonable precautions, encryption, software updates and patches, we cannot guarantee the safety of data transmitted over the internet.