| | |
|---|---|
| POLICY NAME: | Privacy Policy |
| LEAD DIRECTOR: | Peter Hartland |
| LEAD PERSON/AUTHOR: | HR Dept. |
| ORIGINAL APPROVAL DATE: | September 2022 |
| REVIEW / RE-APPROVAL DATE: | September 2023 |

## 1. About this Policy

1.1 St Luke's is committed to protecting the privacy of our employees, volunteers and those that we have contact with. We believe in being open and up front with how we use personal data that is entrusted to us and we are committed to making privacy a Priority.

1.2 We will collect, process, store and share your data safely and securely, by ensuring:

1.2.1 **You're always in control:** Your privacy will be respected at all times and we will put you in control of your privacy with easy-to-use tools and clear choices.

1.2.2 **We work transparently:** We will be transparent about the data we collect and how we use that data so that you can make fully informed choices and decisions.

1.2.3 **We operate securely:** We will protect the data that you entrust to us via appropriate security measures and controls. We'll also ensure that other organisations we work with are just as careful with your data.

1.2.4 **For your benefit:** When we do process your data, we will use it to support you both during the recruitment process and during your employment or involvement with St Luke's.

1.3 The purpose of this Privacy Policy is to provide you with details of exactly what we collect, why we collect and process it, how we look after it, what we do with it.

## 2. Who we are and how you can contact us

2.1. "St Luke's" (also referred to in this policy as "we", "us", "our") is:

**St Luke's Hospice**
Little Common Lane
Sheffield
S11 9NE

| | |
|---|---|
| Registered Company Number: | 0092244 |
| Registered Charity Number: | 254402 |
| ICO Registration Number: | Z8034405 |

## 3. Our Data Protection Officer:

3.1. We have appointed a Data Protection Officer (DPO), who can be contacted in the following ways should you have any questions or feedback about the way your data is handled:

| | |
|---|---|
| Email: | dpo@hospicesheffield.co.uk |
| Mail: | Data Protection Officer<br>St Luke's Hospice<br>Little Common Lane<br>Sheffield<br>S11 9NE |

## 4. How we collect your personal data:

4.1. We collect your personal data in the following ways:

4.1.1. When you apply for a vacancy/ position either internally or externally;

4.1.2. When you apply to volunteer with us;

4.1.3. When you attend an interview;

4.1.4. When we seek references in writing or over the phone;

4.1.5. When you speak to us on the phone or at our offices, shops or events;

4.1.6. When you send emails, letters or social media messages to us;

4.1.7. When we collect data through the implementation of any HR Policies e.g. disciplinary procedures;

4.1.8. In the course of managing your employment with St Luke's, for example, Payroll and Employee Training;

4.1.9. When you use our IT systems or devices.

4.1.10. When we receive your Personal Data from third parties, for example security screening, recruitment agencies, employee benefit providers and HMRC;

4.1.11. Via CCTV that is controlled by St Luke's; and

4.1.12. Via our fob access door management system.

## 5. The data we collect about you:

5.1. We collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

5.1.1. **Identity data** – name, title, date of birth and sometimes your photograph.

5.1.2. **Contact data** – full address, postcode, email address and telephone numbers.

5.1.3. **Next of Kin data** – name, full address, telephone number and relationship information.

5.1.4. **Payment data** – bank account name, number, sort code and bank address.

5.1.5. **Verification data** – Right to work documentation and other security screening information.

5.1.6. **Education and Work History data -** details of your qualifications, skills, experience, employment history and references received.

5.1.7. **Professional Registration data –** register of nurses and doctors who are legally entitled to work in the UK. Using the unique identifying number (PIN) to check the register.

5.1.8. **Insurance data** – to ensure that our doctors have adequate and appropriate insurance or indemnity.

5.1.9. **Performance data** – assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans, details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.

5.1.10. **Usage and Activity data** – employees' use of computers phones, email and the internet in accordance with the terms outlined in the Company Policies that cover these areas. This activity data also include door management and fob access.

5.1.11. **Image data** – images captured by the CCTV controlled by St Luke's.

5.1.12. **Medical & Health Information** – as part of recruitment process, information regarding health and safety at work and absence and sick leave.

5.1.13. **Reference information** – from past employers or character references.

5.1.14. **Expression of Wish** – contact details relating to Death in Service payment recipient.

5.1.15. **Diversity Data –** gender, ethnicity, sexuality and religion for diversity reporting.

5.1.16. **Other Data** – Any other data we legitimately need to collect to comply with your employment contract, to comply with any legal requirements, pursue a legitimate interest of St Luke's or protect St Lukes' legal position in the event of legal proceedings.

## 6. How we use your personal data

6.1. We are only allowed to use personal data about you if we have a legal basis to do so, and we are required to tell you what that legal basis is. We have set out in the table below: the personal data which we collect from you, how we use it, and the legal ground on which we rely when we use the personal data.

6.2. In some circumstances we can use your personal data if it is in our legitimate interest to do so, provided that we have told you what that legitimate interest is. A legitimate interest is when we have a business or commercial reason to use your information which, when balanced against your rights, is justifiable. If we are relying on our legitimate interests, we have set that out in the table below.

| **What we use your personal data for** | **What personal data we collect** | **Our legal grounds for processing** | **Our legitimate interests (if applicable)** |
|---|---|---|---|
| As part of the recruitment and selection process | • CV<br>• Identity<br>• Contact<br>• Reference | • Performance of a contract<br>• Legitimate interest | To ensure that the employee (prospective or contracted) has the right attributes and experience to hold their respective role. |
| To enter into an employment contract with you and manage and maintain our obligations under that contract | • Identity<br>• Contact<br>• Next of Kin<br>• Payment<br>• Verification<br>• Education & Work History | • Performance of a contract<br>• Legal obligation<br>• Legitimate Interest | To ensure that the employee (prospective or contracted) has the right attributes and experience to hold their respective role. |
| Ensure you are legally eligible to work in the UK. | • Identity<br>• Verification | • Performance of a contract<br>• Legal obligation | |
| Verification of your identity as part of pre-employment checks. | • Identity<br>• Contact<br>• Verification | • Performance of a contract<br>• Legitimate interest | To verify the identity of the employee. |

| | | | |
|---|---|---|---|
| Provide you with access to training and development. | • Identity<br>• Contact<br>• Performance | • Performance of a contract<br>• Legitimate interest | To ensure that staff are trained to the appropriate levels. |
| Ensure we can get in touch with you if we need to regarding work or employment related matters. | • Identity<br>• Contact | • Performance of a contract<br>• Legitimate interest | To ensure that staff operate and work safely and efficiently. |
| Ensure we can contact your next of kin in case of an emergency | • Next of Kin data | • Legitimate interest<br>• Vital interest | To ensure you health, safety and security whilst working for us. |
| CCTV recordings | • Image | • Legitimate interest | To ensure your health, safety and security whilst working for us. To assist in investigating performance or conduct at work issues. |
| Health & Safety at work | • Medical and Health<br>• Identity<br>• Contact | • Legal obligation<br>• Vital interests | |
| Diversity reporting | • Diversity data | • Consent<br>• Legal obligation | |
| Door management system | • Activity Data | • Legitimate interest | To ensure your health, safety and security whilst working for us. To assist in investigating performance or conduct at work issues. |

| | | | |
|---|---|---|---|
| Checking your Professional Registrations | • Professional Registration | • Legal obligation<br>• Legitimate interest | To ensure nurses and doctors are legally entitled to work in the UK and in a professional capacity |
| Checking appropriate Indemnity Insurance is in place | • Insurance data | • Legal obligation<br>• Legitimate interest | To ensure doctors have adequate and appropriate insurance or indemnity |
| Recording and executing your Expression of Wish | • Expression of wish data | • Legal obligation<br>• Legitimate interests | To ensure contact is made with the correct person in the event of a death in service |

## 7. Who we share your personal data with

7.1. In order to manage your employment and meet our legal obligations, we only share your data, in the following circumstances:

7.1.1. To manage and maintain the accuracy of your records;

7.1.2. To verify your identity and work history;

7.1.3. To handle Employee/Employer related disputes that may arise;

7.1.4. To handle complaints;

7.1.5. To prevent and detect fraud and other crime;

7.1.6. To allow us to provide you with your contractual benefits administered through third parties;

7.1.7. To meet legal obligations, for example, for the purposes of national security, taxation, criminal investigations, health and safety and statutory audits;

7.1.8. For assessment and analysis purposes to help improve the operation of, and manage the performance of, our organisation;

7.1.9. For any other purpose for which you give us your consent to use your Personal Data; and

7.1.10. When conducting Occupational Health assessments as a new starter or as part of a sickness absence management process.

7.2. We'll never make your personal data available to anyone outside St Luke's for them to use for their own marketing purposes.

## 8. Transferring your personal data outside the EEA

8.1. The EEA is the European Economic Area, which consists of the EU Members States, Iceland, Liechtenstein and Norway. If we transfer your personal data outside the EEA we have to tell you. Please see the table below:

| Purpose of Processing | Nature of the Data | 3rd Party | Location | Safeguard |
|---|---|---|---|---|
| Content Management System for prospective employee data | CV Data | Sitefinity (Progress Software Corporation) | USA | EU-US Privacy Shield |

8.2. Limited personal data that we collect from you may be transferred to and processed in a destination outside of the EEA. In these circumstances, your personal data will only be transferred on one of the following bases:

8.2.1. The country that we send the data is approved by the European Commission as providing an adequate level of protection;

8.2.2. The recipient has agreed with us standard contractual clauses (SCC's) approved by the European Commission, obliging the recipient to safeguard personal data;

8.2.3. There exists another situation where the transfer is permitted under applicable data protection legislation (for example, where a third-party recipient of personal data in the United States has registered for the EU-US Privacy Shield).

8.3. To find out more about how your personal data is protected when it is transferred outside the EEA, please contact our Data Protection Officer. Before sharing any

information with a third party, we will ensure that there is a data sharing agreement in place requiring that the third party protects personal data according to General Data Protection Regulation (GDPR).

## 9. Data Security

9.1. We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

9.2. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator (including the ICO) of a breach where we are legally required to do so.

## 10. How long do we keep your personal data?

10.1. We will only retain your personal data for as long as is necessary to fulfil the purposes for which it is collected. When assessing what retention period is appropriate for your personal data, we take into consideration:

10.1.1. Any statutory or legal obligations;

10.1.2. The requirements of the organisation;

10.1.3. The purposes for which we originally collected the personal data;

10.1.4. The lawful grounds on which we based our processing;

10.1.5. The types of personal data we have collected;

10.1.6. The amount and categories of your personal data; and

10.1.7. Whether the purpose of the processing could reasonably be fulfilled by other means.

10.2. After such time, we will securely delete or destroy your personal data. Below are some examples of the retention periods we have in place:

| Record type | Retention Period |
|---|---|
| Successful recruitment candidate information (including 3rd party referee details provided by the applicant) | 6 years after employment ceases. |
| Unsuccessful recruitment candidate information (including 3rd party referee details provided by the applicant) | 6 months from last action. |
| Personnel files and training records (including disciplinary records and working time records) | 6 years after employment ceases. |
| Redundancy details, calculations of payments, refunds, notification to the Secretary of State | 6 years from the date of redundancy |
| Statutory Sick Pay records, calculations, certificates, self-certificates | 6 years following the end of employment |
| Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence | 3 years after the end of the tax year in which the maternity period ends. |
| Senior executives' records (that is, those on a senior management team or their equivalents) | Permanently for historical reasons |
| Third party emergency contact details provided by the staff member. | Immediately at the end of employment. |
| Pension records | Until the employee reaches age 100. |
| Parental leave | 18 years from the birth of the child |
| Working time records | 2 years from date on which they were made. |
| CCTV Recording | 30 days unless it is part of an ongoing investigation or is relevant to current or expected legal proceedings. |
| Occupational Health records | 6 years after employment ceases. |
| Occupational Health records where termination of employment is due to ill health reasons including stress-related illness incident. | 40 years from date of last entry. |
| Training records relating to safety at work | Permanently |

| | |
|---|---|
| Inland Revenue/HMRC approvals | Permanently |
| Terms and Conditions | 6 years after employment ceases. |
| Termination of employment, for example early retirement, severance or death in service | Until employee reaches age 100. |

## 1. Your rights

1.1. You have certain rights which are set out in the law relating to your personal data. The most important rights are set out below.

1.2. Getting a copy of the information we hold

1.2.1. You can ask us for a copy of the personal data which we hold about you, by writing to the Data Protection Officer (in Section 2). This is known as a data subject access request (DSAR).

1.2.2. You will not have to pay a fee to access your personal data, unless we believe that your request is clearly unfounded, repetitive or excessive. In such circumstances we can charge a reasonable fee or refuse to comply with your request.

1.2.3. We will respond to all legitimate requests within one month.

1.3. Telling us if information we hold is incorrect

1.3.1. You have the right to question any information we hold about you that you think is wrong or incomplete. Please contact the Data Protection Officer if you want to do this and we will take reasonable steps to check its accuracy and, if necessary, correct it.

1.4. Telling us if you want us to stop using your personal data

1.4.1. You have the right to:

1.4.1.1. Object to our use of your personal data (known as the right to object); or

1.4.1.2. Ask us to delete the personal data (known as the right to erasure); or

1.4.1.3. Request the restriction of processing.

1.5. There may be legal reasons why we need to keep or use your data, which we will tell you if you exercise one of the above rights.

1.6. Request a transfer of data

1.6.1. You may ask us to transfer your personal data to a third party. This right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

## 2. Not Happy?

2.1. Please let us know if you are unhappy with how we have used your personal data by contacting the Data Protection Officer (details can be found in section 2).

2.2. You also have a right to complain to the Information Commissioner's Office. You can find their contact details at www.ico.org.uk. We would be grateful for the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.