

Title	Privacy Statement
Category	Corporate Policies
Author(s)	Mark Gillott, Head of IT & Digital
Responsible Director	Tony Saunders, Director of Finance and Chief Operating Officer
Approved by	Amy Stanbridge, September 2025
Date issued	June 2025
Version	1.2
Next review due	June 2027

Version control

Version	Date issued	Brief summary of changes
1	September 2022	Original
1.1	June 2025	Draft – transfer of policy over to new policy template and updated policy scope
1.2	March 2026	Reclassification from policy to statement, with references to policy removed and other minor amendments.

1. Introduction

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 transparent with how we use personal data that is entrusted to us, and we are committed to making privacy a priority.

2. Aims

The aim of this statement is to provide you with details of exactly what data we collect, why we collect and process it, how we look after it and what we do with it.

3. Roles and Responsibilities

St Luke's is committed to ensuring personal data is managed in a secure, lawful, and transparent manner. Responsibility for compliance with this Privacy Statement sits across various roles within the organisation. The **Data Protection Officer (DPO)** holds overall responsibility for monitoring compliance with data protection legislation, responding to data subject requests, advising on privacy matters, and supporting the organisation in managing data protection risks. **Managers and team leaders** are responsible for ensuring their teams understand and follow relevant data protection procedures and for reporting any actual or suspected data breaches. **All staff, volunteers, and contractors** have a responsibility to handle personal data in accordance with this statement and complete the required data protection and information security training.

This document is electronically controlled. The master copy is maintained by the author and stored on the intranet. Once printed, this document becomes uncontrolled. For assurance that the most up to date guidance is being used, staff should refer to the version held on the Intranet.

4. Scope

This privacy statement applies to all personal data processed by St Luke's in the course of managing activities associated with recruitment, selection, onboarding and ongoing administration of staff, volunteers, contractors and applicants.

It covers personal data that we collect and process during recruitment and selection, employee and volunteer engagement, ongoing administration (e.g. absence management, benefits, performance management and payroll) as well as exit processes.

The statement applies to data in all formats and in all locations that St Luke's operates in.

5. About this Statement

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

5.1.1 **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.

5.1.2 **We operate securely:** We will protect the data 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.

5.1.3 **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.

6. Who we are and how you can contact us

6.1 "St Luke's" (also referred to in this statement 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

7. Our Data Protection Officer

7.1 Our Data Protection Officer (DPO) 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
Post:	Data Protection Officer St Luke's Hospice

This document is electronically controlled. The master copy is maintained by the author and stored on the intranet. Once printed, this document becomes uncontrolled. For assurance that the most up to date guidance is being used, staff should refer to the version held on the Intranet.

Little Common Lane
Sheffield
S11 9NE

8. How we Collect your Personal Data

- 8.1 We collect your personal data in the following ways:
 - 8.1.1 When you apply for a vacancy / position either internally or externally.
 - 8.1.2 When you apply to volunteer with us.
 - 8.1.3 When you attend an interview.
 - 8.1.4 When we seek references in writing or over the phone.
 - 8.1.5 When you speak to us on the phone at our offices, shops or events.
 - 8.1.6 When you send emails, letters or social media messages to us.
 - 8.1.7 When we collect data through the implementation of any HR Policies.
 - 8.1.8 While managing your employment with St Luke's, for example, payroll and training.
 - 8.1.9 When you use our IT systems or devices.
 - 8.1.10 When we receive your personal data from third parties, for example security screening, recruitment agencies, employee benefit providers and HMRC.
 - 8.1.11 Via CCTV controlled by St Luke's.
 - 8.1.12 Via our fob access door management system.

9. The Data we Collect about you

- 9.1 We collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:
 - 9.1.1 **Identify data** – name, title, date of birth and sometimes your photograph.
 - 9.1.2 **Contact data** – Full address, post code, email address and telephone numbers.
 - 9.1.3 **Next of kin data** – Name, full address, telephone number and relationship information.
 - 9.1.4 **Payment data** – bank account name, account number, sort code and bank address.
 - 9.1.5 **Verification data** – Right to work documentation and other security screening information.
 - 9.1.6 **Education and work history data** – details of your qualifications, skills, experience, employment history and references received.
 - 9.1.7 **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.
 - 9.1.8 **Insurance data** – to ensure that our doctors have adequate and appropriate insurance or indemnity.
 - 9.1.9 **Performance data** – assessments of your performance, including appraisals, performance reviews, training participated in, performance improvement plans, details of any disciplinary or grievance procedures in which you have been involved in.
 - 9.1.10 **Usage and activity data** – employees use of devices such as phones, computers, email and internet in accordance with the terms outlined in corporate policies that cover those areas. This activity data also includes door management and fob access.
 - 9.1.11 **Reference information** – from past employers or character references.
 - 9.1.12 **Expression of wish** – contact details relating to Death in Service payment receipt.
 - 9.1.13 **Diversity data** – gender, ethnicity, sexuality and religion for diversity reporting.

This document is electronically controlled. The master copy is maintained by the author and stored on the intranet. Once printed, this document becomes uncontrolled. For assurance that the most up to date guidance is being used, staff should refer to the version held on the Intranet.

9.1.14 **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 to protect St Luke's legal position in the event of legal proceedings.

10. How we use your Personal Data

- 10.1 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. The table below sets out the personal data that we collect from you, how we use it, and the legal basis on which we rely when we use the personal data.
- 10.2 In some circumstances we can use your personal data if this 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 • Identity • Contact • Reference	• Performance of a contract • 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 the contract	• Identity • Contact • Next of Kin • Payment • Verification • Education and Work History	• Performance of a contract • Legal obligation • Legitimate interest	To ensure that the employee (prospective or contracted) has the right attributes and experience to hold their respective role.

This document is electronically controlled. The master copy is maintained by the author and stored on the intranet. Once printed, this document becomes uncontrolled. For assurance that the most up to date guidance is being used, staff should refer to the version held on the Intranet.

What we use your personal data for	What personal data we collect	Our legal grounds for processing	Our legitimate interests (if applicable)
Ensure you are legally eligible to work in the UK	• Identity • Verification	• Performance of a contract • Legal obligation	
Verification of your identity as part of pre-employment checks	• Identity • Contact • Verification	• Performance of a contract • Legitimate interest	To verify the identity of the employee
Provide you with access to training and development	• Identity • Contact • Performance	• Performance of a contract • Legitimate interest	To ensure that staff are trained to appropriate levels
Ensure we can get in touch with you if we need to regarding work or employment related matters	• Identity • Contact	• Performance of a contract • Legitimate interest	To ensure that staff operate and work safely and efficiently
Ensure we contact your next of kin in case of an emergency	• Next of Kin data	• Legitimate interest • Vital interests	To ensure your 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

This document is electronically controlled. The master copy is maintained by the author and stored on the intranet. Once printed, this document becomes uncontrolled. For assurance that the most up to date guidance is being used, staff should refer to the version held on the Intranet.

What we use your personal data for	What personal data we collect	Our legal grounds for processing	Our legitimate interests (if applicable)
			conduct at work issues
Health & Safety at work	• Medical and Health • Identity • Contact	• Legal obligation • Vital interests	
Diversity reporting	• Diversity data	• Consent • 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 • 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 • Legitimate interest	To ensure doctors have adequate and appropriate insurance or indemnity

This document is electronically controlled. The master copy is maintained by the author and stored on the intranet. Once printed, this document becomes uncontrolled. For assurance that the most up to date guidance is being used, staff should refer to the version held on the Intranet.

What we use your personal data for	What personal data we collect	Our legal grounds for processing	Our legitimate interests (if applicable)
Recording and executing your Expression of Wish	• Expression of wish data	• Legal obligation • Legitimate interests	To ensure contact is made with the correct person in the event of a death in service

11. Who we share your Personal Data with

- 11.1 To manage your employment and meet our legal obligations, we only share your data in the following circumstances:
 - 11.1.1 To manage and maintain the accuracy of your records.
 - 11.1.2 To verify your identity and work history.
 - 11.1.3 To handle employee / employer related disputes that may arise.
 - 11.1.4 To handle complaints.
 - 11.1.5 To prevent and detect fraud and other crime.
 - 11.1.6 To allow us to provide you with your contractual benefits administered through third parties.
 - 11.1.7 To meet legal obligations, for example, the purposes of national security, taxation, criminal investigations, health and safety and statutory audits.
 - 11.1.8 For assessment and analysis purposes to help improve operation of, and manage the performance of, our organisation.
 - 11.1.9 For any other purpose for which you give us your consent to use your personal data.
 - 11.1.10 When conducting Occupational Health assessments as a new starter or as part of a sickness absence management process.
- 11.2 We'll never make your personal data available to anyone outside St Luke's for them to use for their own marketing purposes.

12. Transferring your Personal Data outside the EEA

- 12.1 The EEA is the European Economic Area which consists of the EU member states, Iceland, Lichtenstein and Norway. If we transfer your personal data outside of the EEA we have to tell you.

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

- 12.2 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 of the following basis:
 - 12.2.1 The country that we send the data to is approved by the European Commission as providing an adequate level of protection.
 - 12.2.2 The recipient has agreed with us standard contractual clauses (SCC's) approved by the European Commission, obliging the recipient to safeguard personal data.
 - 12.2.3 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).
- 12.3 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).

- 12.4 To find out more about how your personal data is protected when it is transferred outside of the EEA, please contact our Data Protection Officer.

13. Data Security

- 13.1 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.
- 13.2 We have put on 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.

14. How long do we keep your Personal Data?

- 14.1 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 will take into consideration:
- 14.1.1 Any statutory or legal obligations.
 - 14.1.2 The requirements of the organisation.
 - 14.1.3 The purposes for which we originally collected the personal data.
 - 14.1.4 The lawful grounds on which we based our processing.
 - 14.1.5 The types of personal data we have collected.
 - 14.1.6 The amount and categories of your personal data.
 - 14.1.7 Whether the purpose of processing could reasonably be fulfilled by other means.
- 14.2 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 3 rd party referee details provided by the applicant)	6 years after employment ceases.
Unsuccessful recruitment candidate information (including 3 rd 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

Record type	Retention Period
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.

15. Your Rights

15.1 You have certain rights which are set out in law relating to your personal data, a summary of which is set out below:

15.2 Getting a copy of the information we hold

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

15.2.2 You will not have to pay a fee for access to 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.

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

15.3 Telling us if information is incorrect

15.3.1 You have the right to question any data 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 it's accuracy and, if necessary, correct it.

This document is electronically controlled. The master copy is maintained by the author and stored on the intranet. Once printed, this document becomes uncontrolled. For assurance that the most up to date guidance is being used, staff should refer to the version held on the Intranet.

15.4 Telling us if you want us to stop using your personal data

15.4.1 You have the right to:

- Object to our use of your personal data (known as the right to object)
- Ask us to delete the personal data (known as the right to erasure)
- Request the restriction of processing.

15.5 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

15.6 Request a transfer of data

15.6.1 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.

16. Not Happy?

16.1 Please let us know if you are unhappy with how we have used your personal data by contacting the Data Protection Officer.

16.2 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.