Title	Data Protection & Information Governance Policy
Category	Corporate
Author(s)	Matt Bruce, Data Protection Officer
Responsible Director	Tony Saunders, Director of Finance and Chief Operating Officer
Approved by	Amy Stanbridge, October 2025
Date issued	June 2025
Version	3.2
Next review due	June 2027

Version control

Version	Date issued	Brief summary of changes
1.0	15/05/2018	Matt Bruce – new policy drafted
2.0	15/03/2020	Matt Bruce – Merged information governance policy
3.0	19/05/2021	Matt Bruce – Update to legislation – "GDPR" to "UK GDPR"
3.1	24/05/2021	Matt Bruce – Minor changes following TS review
3.2	13/06/2025	Mark Gillott - Minor changes to comply with new policy template. Changes to roles and responsibilities to reflect organisational changes.

1. Introduction

St Luke's understands the importance of ensuring and maintaining the safety and security of personal data and it is of paramount importance to ensure that information is effectively and efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

This supports and ensures our continued compliance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and alignment with the NHS Data Security and Protection Toolkit.

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the NHS National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal data is handled correctly.

St Luke's needs to collect and process personal data about the people we work with, including our employees, volunteers, supporters and patients, in order to effectively and compliantly carry out our everyday organisational functions and to provide our services. In addition, we may occasionally be required by law to collect and use certain types of personal data and special category data to comply with the requirements of the law.

This data can include (but is not limited to), name, address, email address, date of birth, IP address, identification number, private and confidential information, special category data (including medical and health information) and bank details.

We are committed to collecting, processing, storing and destroying all information in accordance with relevant data protection laws.

This information in this document is subject to regular review by our Data Protection Officer (DPO).

Key definitions within this policy can be found in Appendix 1.

2. Policy Aims / Objectives

This policy aims to ensure that we are meeting, and continue to meet, our legal, statuary and regulatory requirements under applicable Data Protection laws and to ensure that all personal and special category data is safe, secure and processed compliantly whilst in use and/or being stored and shared by us.

St Luke's recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. It fully supports the principles of corporate governance and recognises its public accountability as a charity, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

It also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

St Luke's believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such, it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

3. Policy Scope

This policy relates to:

- All permanent, fixed term and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, supporters, patients, apprentices, interns and agents engaged with St Luke's
- All personal and/or special category data that is obtained, stored or otherwise processed by St Luke's.

4. Roles and Responsibilities

4.1 Chief Executive

The Chief Executive has overall accountability and responsibility for governance, including information governance at St Luke's. The Chief Executive delegates the operational oversight of information governance to the Senior Information Risk Owner (SIRO)

4.2 Senior Information Risk Owner (SIRO)

The Director of Finance and Chief Operating Officer is the nominated SIRO of the Executive. They will take strategic lead for information governance and will:

- Understand how the strategic business goals of St Luke's may be impacted by information risks
- Act as an advocate for information risk on the Board of Trustees; and
- Ensure that identified information security threats are followed up and incidents managed.

4.3 Caldicott Guardian (CG)

The Head of Clinical Governance is St Luke's Caldicott Guardian and has specific responsibilities in relation to clinical information to:

- Justify the purpose(s) for using confidential information
- Only use it when it's necessary
- Use the minimum information that is required
- Provide access and share information on a strict need-to-know- basis
- Ensure everybody understands their responsibilities relating to confidentiality
- Understand and comply with the law.

4.4 Head of IT & Digital

The Head of IT & Digital acts as the day-to-day operational lead for information governance by:

- Providing advice and guidance to staff on data protection, information security and records management matters
- Supporting and advising on information security aspects of projects and new initiatives
- Ensuring that appropriate technical and organisational controls are in place to safeguard personal data
- Supporting in the completion of Data Protection Impact Assessments (DPIAs) and providing advice on information security risk mitigations
- Ensuring that systems used for processing personal data are compliant by design and by default
- Monitoring compliance with information governance policies and report on risks, issues and improvements to the Exec
- Promoting a culture of data protection and privacy awareness, including contributing to training and awareness initiatives
- Escalating to the DPO when required.

4.5 Data Protection Officer (DPO)

The DPO is responsible for monitoring compliance with applicable Data Protection laws. This includes;

- Raising awareness of Data Protection within our organisation and overseeing and conducting staff training
- Cooperating with, liaising and reporting to the UK's Supervisory Authority (the Information Commissioner's Office)
- Maintaining independence, avoiding conflicts of interest with operational roles
- Acting as an escalation point for high-risk or non-compliance issues to the Exec and governance committees
- Acting as the main contact point to the Supervisory Authority and Data Subjects when they make a request or contact St Luke's in relation to personal data.

The Data Protection Officer can be contacted by emailing dpo@hospicesheffield.co.uk

4.6 Information Asset Owners (IAO)

- The **Exec Lead for Care** has overall responsibility for all patient related nursing care and allied health professional records
- The **Exec Lead for Strategic & Competitive Performance** has overall responsibility for any records or information relating to marketing activity

- The **Head of Fundraising** has overall responsibility for any records or information relating to fundraising activity
- The **Director of People and Wellbeing** has overall responsibility for all staff and volunteer records
- The **Director of Finance and Chief Operating Officer** has overall responsibility for all financial, payroll and business operation records and will ensure that they are held securely and will be available for internal or external scrutiny and audit. In conjunction with the **Head of Operations, Purchasing** and the **Head of IT & Digital** they also have overall responsibility for all estate, building, IT and statutory related records.

All of the above parties are collectively the **Information Asset Owners (IAO)** for their defined areas of responsibility. Their principle role are to:

- Understand and address risks to the information assets they own
- Provide assurance to the **SIRO** and **Data Protection Officer** on the security and use of these assets
- Ensure that any service developments or changes adequately consider information governance and information risk. Wherever there are residual risks specialist advice should be sought from the **IT Department**, **Data Protection Officer** and **Clinical Quality and Risk Lead**
- Ensure that periodical and routine audits, inspections and spot checks are undertaken with regard to the security, quality and completeness of the records within their defined areas of informed responsibility.

5. Training Requirements

All staff must complete mandatory information security training upon joining St Luke's and at regular intervals thereafter. Refresher training will be provided annually or when significant changes to data protection laws or organisational processes occur.

Additional role specific training may be required for staff who handle sensitive or large volumes of personal data, or who are involved in data processing activities.

People that hold dedicated roles relating to data protection and information governance will also undertake role specific training.

6. The Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest.

The legislation that they have oversight of includes:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- The Privacy and Electronic Communication Regulations 2003 (PECR)
- Freedom of Information Act 2000 (FOI)
- The Environmental Information Regulations 2004.

Under the GDPR, the ICO as the UK's Supervisory Authority, can issue enforcement notices and fines for breaches if any of the Regulations, Acts and/or Laws regulated by them.

St Luke's is registered with the ICO and appear on the Data Protection Register as a **Data Controller** of personal data. St Luke's ICO Registration number is: **Z8034405.**

7. What is UK GDPR?

The UK General Data Protection Regulation (UK GDPR) provides individuals with more control over their personal data and ensures transparency and accountability with regards to how their personal data is processed. UK GDPR requires that appropriate security and controls are in place to protect personal data. St Luke's understands and supports the principles are set out in Article 5 of the UK GDPR that require personal data be:

1. Processed **lawfully, fairly** and in a **transparent** manner in relation to individuals (lawfulness, fairness and transparency).
2. Collected for **specified, explicit** and **legitimate** purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).
3. **Adequate, relevant** and **limited** to what is **necessary** in relation to the purposes for which they are processed (data minimisation).
4. **Accurate** and, where necessary, kept **up to date** (accuracy).
5. Kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed (storage limitation).
6. Processed in a manner that ensures **appropriate security** for the personal data (integrity and confidentiality).

Article 5 (2) states that the controller shall be responsible for, and be able to demonstrate compliance with, the principles (the **accountability** principle). This principle requires both data controllers and data processors to document and record their processing activities to show how they comply with the UK GDPR.

8. Lawful Processing Conditions

Article 6 of the UK GDPR defines the lawful bases for processing. Prior to carrying out any processing activity on personal data, St Luke's will always identify and establish the legal basis for processing and verify this with the regulation. We will not process any personal data unless one of the following conditions are met:

1. **Consent -** The data subject has given consent to the processing of their personal data for one or more specified purposes.
2. **Performance of a Contract** - Processing is necessary for the performance of a contract to which the data subject is party.
3. **Performance of Legal Obligation** - Processing is necessary for compliance with a legal obligation to which the data controller (St Luke's) is subject.
4. **Vital Interests** - Processing is necessary in order to protect the vital interests (life or death situation) of the data subject or of another natural person.
5. **Public Task** – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (St Luke's).
6. **Legitimate Interests** - Processing is necessary for the purposes of legitimate interests pursued by the controller (St Luke's) or by a third party.

8.1 Consent

Where any of our processing activities rely on the data subjects' consent (such as marketing preferences), we will ensure that we collect their consent in accordance with UK GDPR. Under UK GDPR, consent must be:

- **Freely given** – the data subject must have a genuine choice, and where there is an imbalance of power between the data controller and the data subject, for example employer and employee, consent cannot be considered freely given
- **Specific** – the data controller must explain its purpose(s) for the processing of the personal data so that the data subject can consent to the purpose(s) specifically
- **Informed** – the data subject must be given all necessary details of the processing activity so that they can comprehend how the processing might affect them
- **An unambiguous indication** – the data subject's statement or clear affirmative action must leave no doubt as to their intention to give consent
- **A clear affirmative action** – the consent is given on an opt-in basis, for example an unticked box which the data subject can then tick themselves.

St Luke's maintain auditable records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable.

We also ensure that the data subject can withdraw their consent as easily as they managed to give it, and where their consent is withdrawn, we will respect their wishes.

8.2 Legitimate Interests

If we rely on legitimate interests as our lawful condition for processing, then we will be transparent with the data subject about what our legitimate interests are.

We will take into consideration how the data subject may reasonably expect us to use their personal data, and we will cease to process their personal data where the rights of the data subject override our legitimate interests, in particular where the data subject is a child. The DPO will perform a Legitimate Interest Assessment (LIA) when taking all factors into consideration.

9. Objectives

To help us meet the regulatory requirements of applicable data protection law and alignment with the Data Security & Protection Toolkit, we have developed a set of objectives.

St Luke's will:

- Develop, implement and maintain policies and procedures governing the collection, processing and disposal of personal data to ensure they are in accordance with applicable data protection laws
- Only obtain, store and process personal data when we have a valid, lawful basis for doing so
- Monitor all organisational practices for compliance with applicable data protection laws
- Record and maintain our processing activities as evidence of compliance with the accountability principle
- Ensure that all employees are provided with data protection and information governance training so that they are aware of their responsibilities and obligations with regards to our organisation

- Be open and transparent with our supporters, volunteers, donors, employees and patients so that they feel confident and secure when providing us with their personal data, knowing that it will be processed in compliance with applicable data protection laws
- Continually review our business practices and policies with regards to applicable data protection laws to identify any non-compliance issues before they become a risk
- Protect the rights of data subjects provided to them by applicable data protection laws and ensure that we have suitable facilities in place to help data subjects exercise their rights.

10. Data Subject Rights

Data subjects have the following rights under UK GDPR:

1. The right to be informed
2. The right to access
3. The right to rectification
4. The right to erasure (also known as the 'right to be forgotten')
5. The right to restriction of processing
6. The right to data portability
7. The right to object to processing.

Per Article 22 of the UK GDPR, an individual also has 'the right not to be subject to a decision based solely on automated decision making, including profiling, which produces legal effects concerning them or similarly significantly affects them'.

11. Privacy Notices

Before we collect an individual's personal data, St Luke's will ensure that we have provided them with the required information according to Articles 13 and 14 of the UK GDPR, known as 'fair processing information'.

Where the personal data has not been collected directly from the data subject, we will ensure that the data subject is also informed about the source we used to obtain their personal data.

Our fair processing information is contained within our privacy notices and we have taken every step to ensure that this information is:

- concise
- transparent
- intelligible
- easily accessible
- written using clear, plain language.

In particular, when the fair processing information is intended for children or individuals with educational needs, we will ensure that they can understand the information.

We will provide the following information:

- The identity and contact details of the data controller (St Luke's) as well as the contact details of our DPO
- The purposes of processing and the legal basis for processing
- The recipients, or categories of recipients, of the personal data
- Whether or not we intend to transfer the personal data to a third country or international organisation, and the safeguards we have in place if we choose to do so
- How long we intend to keep the personal data (retention period) or the criteria used to determine the retention period
- The existence of the data subjects' rights, including the right to lodge a complaint with the UK's supervisory authority (the ICO)
- Whether the provision of the personal data is a statutory or contractual requirement and the possible consequences of not providing the data
- The existence of any automated decision making.

12. Data Subject Access Requests (DSARs)

St Luke's facilitates data subjects' right to access any personal data we hold or process about that individual. We will endeavour to supply a data subject with their personal data within one month of receiving their request. Our procedure for handling a subject access request is detailed in our *Data Subject Access Request Policy*.

13. Data Retention

In accordance with the storage limitation principle, St Luke's will not keep an individual's personal data for longer than necessary. We have specified retention periods and disposal methods for all categories of personal data that we process, and these can be found in our *Records Retention and Disposal Policy*.

14. Data Quality

All Patient Care Staff or Support Staff who use, add to or amend clinically related records are responsible for the quality, integrity and confidentiality of those records. This includes the filing of reports, ensuring that duplication of patient information is avoided, that the notes are filed in template and chronological order.

15. Data Sharing

St Luke's does not share personal data with any countries outside of the European Economic Area (EEA) unless that country has been given an adequacy decision by the European Commission ensuring that they can provide a suitable level of protection for personal data, or they can demonstrate that they have implemented the appropriate safeguards, such as:

- Binding corporate rules (BCRs) in place.
- Having Standard Contract Clauses (SCCs) in place, imposing obligations on the third party to protect the rights and freedoms of the data subjects.

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 and safeguards personal data in line with UK GDPR. All data sharing will be transparently reflected in our privacy notices.

16. Data Protection by Design

We are proud to operate a data protection by design approach to the protection of personal data and we consider the safety and security of the personal data that we hold in every processing activity we undertake, from the beginning right through to completion. Privacy and protection of information is a key consideration of during the life cycle of a project or activity affecting a subject.

This approach means that:

- We are able to identify any issues concerning our processing activities and take action before they become a risk;
- There is an increased awareness of data protection across our organisation;
- We are able to demonstrate how we comply with UK GDPR in accordance with the accountability principle;
- Actions we take are less likely to have a negative impact on the privacy of data subjects.

Our data protection by design approach to protecting personal data ensures the security of data that is processed, especially when it is shared, disclosed and transferred. We implement appropriate technical and organisational measures recommended by UK GDPR, including:

- Pseudonymisation
- Encryption
- Data minimisation
- Restriction.

Our *Information Security Policy* provides more detailed information about the measures and controls that we take to protect personal information and to ensure its security from the time it is collected to its disposal.

17. Data Protection Impact Assessments

Before we begin any new processing activities, we will carry out a Data Protection Impact Assessment (DPIA) and, from time to time, consult with our DPO. We will undertake a DPIA particularly in the case of:

- Systematic and extensive evaluations of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal or other significant effects on the data subject
- Processing special categories of data on a large scale, or personal data relating to criminal convictions and offences
- Systematic monitoring of data subjects on a large scale (e.g. CCTV).

More information about DPIAs and the procedure for carrying out a DPIA is available in our *Data Protection Impact Assessments Policy*

18. Penalties

St Luke's understands that any infringements on the UK GDPR are likely to result in action taken by the ICO, including possible fines. We recognise that:

- We may be fined up to £8.7 million pounds, or 2% of annual turnover (whichever is higher) for infringements concerning; -
    - The obligations of the controller and processor;
    - The obligations of the certification body;
    - The obligations of the monitoring body.

- We may be fined £17.5 million or 4% of annual turnover (whichever is higher) for infringements concerning; -
    - The basic principles for processing, including conditions for consent;
    - The data subjects' rights;
    - Transfers of personal data to a recipient in a third country or an international organisation;
    - Any obligations pursuant to UK law;
    - Non-compliance with an order from the supervisory authority (the ICO)

19. Data Breach Management

St Luke's understands that every data protection incident should be recognised and handled appropriately. This is the responsibility of every employee within the organisation. St Luke's employees recognise that:

- All data protection incidents should be reported to their Line Manager and the DPO. Please see the *Data Breach Management Policy* for more information.

- Where the DPO deems any incident to be classified as a major incident, which significantly impacts the rights and freedoms of the Data Subject, then it must be reported to the Supervisory Authority (ICO) by the DPO within 72 hours.

- The DPO will inform the Executive Team, who will then notify the Trustees immediately upon classifying any breach as a major incident, prior to notification to the ICO.

More information about Data Breach Management is available in our *Data Breach Management Policy*

Appendix 1

Definitions

Personal data means any information relating to an identified or identifiable natural person ('data subject').

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data subject means an individual who is the subject of personal data.

Data controller means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Third Party means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Supervisory Authority means an independent public authority which is established by a Member State.