St Luke's
for flourishing, healthy clergy

Data Protection Policy

2021

Background

The General Data Protection Regulation (GDPR) became effective in the UK in May 2018. It is enshrined in UK law by the Data Protection Act 2018 (DPA) which replaces the previous Data Protection Act 1998 and gives individuals more rights and protection over how their personal data is used by organisations. GDPR and DPA are enforced by the Information Commissioner, operating through the Information Commissioner's Office (the ICO). The ICO publishes guidance and has a broad range of powers, including the ability to issue fines for breaches.

Description of St Luke's data processing activities

St Luke's regularly processes the following categories of personal data:

Staff: St Luke's has a small number of employees, about whom it holds personal data such as employment history, education and qualifications, and identifiers such as contact details and record of employment with St Luke's. Very occasionally, St Luke's may process information about its employees' health or medical details. St Luke's processes such employee personal data for ordinary staff administration purposes, including salary payment and conferring other benefits, conducting appraisals, training, and management. It also collects personal data about prospective candidates in the recruitment process. St Luke's holds some information about its employees and former employees for archival and historical research purposes.

Beneficiaries: In order to further its charitable aims, St Luke's processes personal data about beneficiaries and potential beneficiaries, which may include personal, family, and medical information. St Luke's may also process personal data about its beneficiaries for historical and archiving purposes.

The public: St Luke's may enter into correspondence with members of the public, such as donors, clergy, diocesan staff, and members of Parochial Church Councils (PCCs). When it does so, St Luke's may collect incidental personal data such as contact details, and it processes such personal data in order to respond to queries and donations.

Suppliers: St Luke's processes personal data concerning its suppliers of goods and services, including identifiers such as contact details, financial information, and purchase history. St Luke's processes such information in order to purchase goods and services, to pay its suppliers and to maintain its accounts and records.

This policy does not document every part of the Data Protection Legislation which may be relevant, but merely focuses on the key aspects that are likely to be applicable to St Luke's. Should other issues arise in practice not covered by this policy, St Luke's will consider these separately at the time. St Luke's will review this policy annually and may amend it from time to time as it sees fit.

1. Applicable data protection law

In this policy, any reference to Data Protection Legislation means the Data Protection Act 2018 (DPA) or the GDPR.

2. Key concepts of applicable data protection law

The Data Protection Legislation relies on a number of key definitions, which are explained below.

'***personal data***' means any information relating to an identified or identifiable natural person (a 'data subject', which is explained in more detail below). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the identity of that natural person.

St Luke's will hold personal data about its past, present, and prospective supporters, staff, and members of the public such as beneficiaries, as well as its suppliers. St Luke's may hold such personal data both in electronic and hard copy format, in records, correspondence and minutes.

'***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. Processing is interpreted very broadly, so that almost all activities which organisations carry out in relation to their personal data are captured by the definition.

St Luke's will generally be deemed to be processing any personal data that it may collect, record, store and/or disclose.

'***controller***' means the natural or legal person, public authority, agency, or other body, which determines the purposes and means of the processing of personal data. The Data Protection Legislation applies to controllers, who must comply with its requirements.

The Chief Executive will generally be the controller in relation to the personal data of Trustees, staff, members of the public such as beneficiaries and enquirers, and suppliers.

'***processor***' means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller. Where a controller uses a processor to process personal data on his her or its behalf, the controller must only use a processor that provides sufficient guarantees to ensure that personal data is processed securely, and in accordance with the requirements of the GDPR. Controllers must engage processors by way of a contract incorporating the provisions specified by Article 28 of the GDPR.

St Luke's may use processors for a variety of purposes; for instance, to store personal data, to send email communications, or to calculate staff payroll. In each case, it must have conducted sufficient due diligence to be able to evaluate whether the processor offers sufficient guarantees to protect personal data and must ensure that the processor is bound by a contract that incorporates the provisions specified by the GDPR. The requirements around appointing processors are explained in more detail below (see Third Party Processors section).

'***special categories of personal data***' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health (including medical data, and medical records, for example), or concerning an individual's sex life or sexual orientation. Special categories of personal data is the term used in the GDPR which, broadly speaking, replaces the concept of 'sensitive personal data' from the DPA.

The special categories of personal data require a higher standard of care. If a personal data breach (as defined below) occurs that involves the loss of any of the special categories of personal data, the ICO will regard this as a serious breach. The GDPR also requires that personal data relating to criminal convictions and offences is treated with a higher standard of care.

Due to the nature of the work that St Luke's undertakes, the charity is required to store a limited amount of special category data such as medical information of potential beneficiaries to support their request to become a beneficiary e.g. referral letters from GPs.

'***data subject***' means an individual to whom personal data relates. Typically, these are employees, customers, and suppliers.

The categories of data subject whose personal data St Luke's is likely to process will include Trustees, staff, beneficiaries, suppliers, and members of the public.

'***personal data breach'*** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach may be accidental, such as a system failure, or loss of an electronic or physical file, or malicious, such as a cyberattack. In the event that St Luke's suffers a personal data breach, it must take specific steps, explained below in this policy.

3. The data protection principles

The data protection principles are standards that St Luke's must observe when processing personal data. These principles are as follows:

i. Fairness, lawfulness and transparency

This is the most important of the data protection principles and comprises three elements; fairness, lawfulness and transparency. Considering these in more detail:

Fairness: Organisations generally cannot process individuals' personal data in a way that an individual would not have reasonably expected. Collecting personal data on the pretext of one purpose and then using it for another, unrelated purpose is unlikely to be fair. St Luke's should consider whether its uses of personal data would fall within the reasonable expectations of the affected data subjects.

Transparency: Organisations must provide certain prescribed information to individuals when processing their personal data, including the organisation's identity, the purposes for which personal data is being processed, or is to be processed, and any third-party recipients of the personal data. A complete list of the information that must be provided to data subjects can be found in Articles 13 and 14 of the GDPR. The transparency information must accurately reflect the controller's use of personal data. This is frequently provided by way of a website privacy notice but may also be provided by way of a disclaimer on a paper form, or a pre-recorded message in the context of recorded telephone calls.

St Luke's must ensure that its website privacy notice, and any other means by which it makes the transparency information available to data subjects (such as a disclaimer on a paper form) accurately and comprehensively reflects its processing activities.

Lawfulness: Organisations must establish at least one of a number of lawful grounds for processing. These lawful grounds are set out in Article 6 of the GDPR and are as follows:

1) The data subject has given his or her **consent** to the processing. Note that to be valid, consent must be freely given, informed (by way of the transparency notice, explained above) specific, and capable of withdrawal at any time, without detriment to the data subject. Consent must be indicated by way of an unambiguous, positive affirmation by the data subject. Consent cannot be inferred from the absence of an objection and will not be valid where the data subject does not have a genuine choice.

2) Processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.

3) Processing is necessary for **compliance with a legal obligation** to which the controller is subject.

4) Processing is necessary in order to protect the **vital interests of the data subject** or of another person.

5) 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.

6) Processing is necessary for the purposes of **legitimate interests** pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.

In practice, St Luke's will frequently be able to rely on the second and sixth grounds (performance of a contract, and the legitimate interests ground) for many of its activities. Note that the grounds for processing the special categories of personal data are different.

ii. Purpose limitation

This principle requires that the purposes for which personal data is processed are limited to those purposes specified in the transparency information that has been provided to the affected data subjects, and not processed for any further, incompatible purposes. Note that any further processing operations for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible purposes.

St Luke's will only process personal data it holds for those purposes specified in the website privacy notice or other such transparency notice.

iii. Data minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. St Luke's will only collect the personal data that is strictly necessary for the purpose for which it was collected, and will not collect additional, unnecessary personal data on a 'just in case' basis.

iv. Accuracy

Personal data must be kept accurate and up to date. St Luke's must ensure that any requests from data subjects to update their personal data are dealt with promptly, having satisfied itself as to the requester's identity.

v. Storage limitation

The starting point for GDPR and DPA is that personal data must not be kept for longer than is necessary for the purposes for which the data are processed. In reality the duration for which personal data is stored will be dictated by applicable legal, business or other reasons, such as tax legislation.

If St Luke's cannot establish a valid legal, business or other reason for retaining personal data, it must be securely deleted. After the applicable legal storage period for medical records and financial records has expired, personal data will be deleted.

vi. Integrity and confidentiality

Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

St Luke's will take appropriate measures that are proportionate to the risk associated with the personal data it holds. Such measures may be technical, such as password protection of laptops, or organisational, for example, by operating a layered access policy, appropriate vetting of staff who have access to personal data, conducting appropriate due diligence on any third parties that process personal data on St Luke's behalf, and binding them by an appropriate engagement contract.

vii. Accountability

Controllers are responsible for compliance with the principles explained above and must be able to demonstrate compliance, with appropriate evidence.

4. Data subjects' rights

Data Protection Legislation confers a number of rights upon data subjects, which controllers must observe. Data subjects' rights are a cornerstone of Data Protection Legislation and must be dealt with promptly should one arise. St Luke's is unlikely to receive data subject requests on a regular basis so this Policy does not go into detail, but St Luke's must be able to recognise a request from a data subject to exercise his or her rights. The most relevant of these rights, from St Luke's perspective, are summarised below:

i. Data subject access requests

Data subjects are entitled to access their personal data held by St Luke's on request (Article 15 GDPR). The response to a data subject access request must include certain information, such as: the purposes of the processing; the recipients (or categories of recipient) to whom the personal data have or will be disclosed; and individuals' rights to have their data corrected, deleted or to restrict the processing of their data.

Note that under the GDPR, the information must be provided to data subjects free of charge and within one month of the request. This differs from the previous position, under the DPA, which allowed an organisation to charge a fee of up to £10 for dealing with a request, and the response period was 40 days.

ii. The right to be forgotten

Data subjects have the right to request St Luke's erase all data held in respect of them in various circumstances (Article 17 GDPR). However, the right to be forgotten is not an absolute right, and St Luke's is only obliged to give effect to a request in a number of specific situations, the most relevant of which are likely to be:

1) Where the purpose for which the personal data was processed no longer applies; or

2) Where St Luke's processing of the personal data is based on consent and the data subject withdraws his or her consent.

iii. The right to rectification

Data subjects have the right to have incorrect personal data about them corrected without undue delay (Article 16 GDPR).

St Luke's must endeavour to ensure that any personal data it processes is up to date and correct. Where an error or inaccuracy is discovered, St Luke's should correct this as soon as possible.

iv. The right to data portability

Data subjects have the right, in certain circumstances, to access their data in machine-readable format and, where technically possible, to have their data transferred directly from St Luke's to another data controller (Article 20 GDPR).

v. The right to object

Data subjects have the right, in a number of specific circumstances, to object to having their personal data processed (Article 21 GDPR). The most relevant of these circumstances is where the processing is based on St Luke's legitimate interests (explained in section 3(i)(6) above). Data subjects may also object to their personal data being processed by St Luke's for direct marketing purposes.

5. Other requirements

St Luke's must process personal data in accordance with the principles explained above. However, the Data Protection Legislation imposes a number of additional requirements, which are explained below.

i. Breach notification

The ICO expects St Luke's to have a documented data protection breach procedure in place. In the event of a data protection breach, the ICO would regard the absence of a breach management plan as an aggravating factor. St Luke's has a Data Protection Breach Procedure that is reviewed and updated annually.

Reporting breaches to the ICO

Under the GDPR, if a data security breach occurs, St Luke's (as controller) must notify the breach to the ICO without undue delay and, where feasible, within 72hrs of the personal data breach occurring. However, this notification requirement does not apply where the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.

This is covered in detail in the St Luke's Data Protection Breach Procedure.

Reporting breaches to individuals

Where a data security breach occurs, and it is likely to result in a 'high risk' to the rights and freedoms of the individuals concerned, St Luke's must notify the affected individuals 'without undue delay'. However, St Luke's is not required to notify data subjects if:

1) The personal data concerned had been rendered unintelligible (for example, by way of encryption); or
2) Subsequent measures have been taken by St Luke's so that there is no longer a high risk to the individuals; or
3) It would involve disproportionate effort to communicate to each affected data subject individually, although where this applies then a general public communication must be made.

This is also covered in the Data Protection Breach Procedure. St Luke's must maintain a schedule of data breaches (whether or not notification was made at the time), to comply with GDPR.

ii. Data protection impact assessments (DPIAs)

A DPIA consists of a documented consideration and evaluation of the data protection risks arising from a proposed new processing activity, along with recommended mitigation strategies to address the risks.

Under Article 35 of the GDPR, St Luke's is required to undertake a DPIA 'where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural people.

St Luke's does not believe that the nature of its processing is such that there is likely to be a high risk to the rights and freedoms of the data subjects whose personal data it holds. As a result, St Luke's does not believe that it is necessary for it to undertake any DPIAs at present. St Luke's will keep this under review, including reviewing any guidance issued from the ICO.

iii. Third party processors

The rules around the appointment of processors (the meaning of which is explained in Section 2, above) are strict, and amount to an organisational security measure. In the event that St Luke's were to suffer a personal data breach involving a third-party processor, the ICO would expect to see that appropriate due diligence had been conducted on that provider and that the appropriate contract was in place.

Before the GDPR came into force, St Luke's ensured that it had a written contract which met the requirements of GDPR in place with each processor it used. St Luke's only uses processors that agree that they will meet the requirements of the GDPR and will protect data subjects' rights.

Before engaging a processor, St Luke's checks that the processor has appropriate technical and organisational measures in place to keep data secure; and that the processor's staff who will be engaged in processing personal data on behalf of St Luke's are subject to a duty of confidentiality and receive regular training in data protection matters.

St Luke's regularly reviews the activities and processes of the processors it uses, to check that the processor is processing personal data in line with its internal processes and is complying with relevant requirements under the Data Protection Legislation and its contractual commitments in respect of the personal data.

6. Further information

For further information about this policy and St Luke's data handling practices, please contact:

Claire Walker
Claire.walker@stlukesforclergy.org.uk

St Luke's Healthcare for the Clergy
Room 201, Church House
27 Great Smith Street
London
SW1P 3AZ
T: 020 7898 1700
www.stlukesforclergy.org.uk

7. Responsibility

Overall responsibility for this policy and its implementation lies with the Board of Trustees.

8. Review

This policy is reviewed annually and updated as required.

Approved by the Trustees 19th March 2021.