ST JOHN'S & ST PAUL'S

General Data Protection Regulation

APRIL , 2023

ST JOHN'S & ST PAUL'S
Greenway Road, Widnes, Cheshire. WA8 6HA

St John's and St Paul's

Contents

1 Aim and scope of policy

This policy applies to the processing of personal data in manual and electronic records kept by St John's and St Paul's, in connection with its human resources function as described below. It also covers St John's and St Paul's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade

union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is 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.

St John's and St Paul's makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with General Data Protection Regulation (GDPR) and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of St John's and St Paul's, St John's and St Paul's will ensure that the third party takes such measures in order to maintain St John's and St Paul's commitment to protecting data. In line with current data protection legislation, St John's and St Paul's understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Throughout this document, there are three roles involved in the GDPR process.

GDPR role 1 is the GDPR processor who handles peoples' details and any requests for those details held.
This is the Church Administrator. (in 2023 this is Felicity Price).

GDPR role 2 is the Data Protection Reviewer as described in 8 below.
This is the Finance and Operations Manager (in 2023 the post holder is Tim Mason).

GDPR role 3 is the Data Protection OfficerChurch Warden, as described in 7 below.
This is one of the Church Wardens. (in 2023 this is Gwen Evans)

2 Types of data held

Personal data is kept in personnel files or within St John's and St Paul's Human Resource (HR) systems.

The following types of data may be held by St John's and St Paul's, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

Relevant individuals should refer to St John's and St Paul's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

2.1 Data protection principles

All personal data obtained and held by St John's and St Paul's will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant data protection procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability

- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

2.2 Procedures

St John's and St Paul's has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these different roles.

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by St John's and St Paul's
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. St John's and St Paul's understands that consent must be freely given, specific, informed and unambiguous. St John's and St Paul's will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences

3 Access to data

Relevant individuals have a right to be informed whether St John's and St Paul's processes personal data relating to them and to access the data that St John's and St Paul's holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from the Church Administrator **.** The request should be made to the Church Administrator.
- St John's and St Paul's will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- St John's and St Paul's will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform St John's and St Paul's immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. St John's and St Paul's will take immediate steps to rectify the information.

For further information on making a subject access request, contact the Church Administrator.

3.1 Data disclosures

St John's and St Paul's may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

4 Data security

St John's and St Paul's adopts procedures designed to maintain the security of data when it is stored and transported.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- refrain from sending emails containing sensitive work-related information to their personal email address
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Church Administrator. Where personal
data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow St John's and St Paul's rules on data security may be dealt with via St John's and St Paul's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

4.1 International data transfers

St John's and St Paul's does not transfer personal data to any recipients outside of the UK.

4.2 Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of

individuals, it will be reported to the Information Commissioner within 72 hours of becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, St John's and St Paul's will do so without undue delay.

5 Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for St John's and St Paul's are trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and St John's and St Paul's of any potential lapses and breaches of St John's and St Paul's policies and procedures.

6 Records

St John's and St Paul's keeps records of its processing activities including the purpose for the processing and retention periods in its HR data record. These records will be kept up to date so that they reflect current processing activities.

7 Data Protection Officer

St John's and St Paul's Data Protection Officer is **GDPR Person 3** (Oversight and Effectiveness/Integrity Officer.

8 Data Protection Reviewer and Auditor (of GDPR systems and procedures) **GDPR Person 2**