Data Protection Policy

Purpose

The purpose of this policy is to describe the steps that the Parochial Church Council of All Saints' Preston on Tees ('the PCC') are taking to comply with data protection legislation, to ensure that our compliance with the relevant legislation is clear and demonstrable.

Name	Matt Levinsohn	**Position:**	Chair of PCC, Vicar
Signature		**Date:**	18th March 2024

Contents

1 Introduction

1.1 Purpose

The purpose of this policy is to describe the steps that the Parochial Church Council of All Saints' Preston on Tees ('the PCC') are taking to comply with data protection legislation, to ensure that our compliance with the relevant legislation is clear and demonstrable.

This policy is also intended to define measures for ensuring that risks to individuals through misuse of personal data are minimised, such as:

- personal data being used by unauthorised individuals through poor security or inappropriate disclosure;
- individuals being harmed by decisions made using inaccurate or insufficient data;
- individuals not being informed about how their information is being used due to a lack of transparency
- individuals not being notified of data breaches and other unlawful practices impacting their personal data;
- the invasion of privacy due to over-collection or over-retention of data.

1.2 Scope & Application

The scope of this policy covers personal data that All Saints' Preston on Tees collects, uses, stores, transfers, and shares to protect individual rights with respect to that data (Appendix 1). We expect all those processing personal data on behalf of All Saints' Preston on Tees to act in accordance with this policy when engaged in the business of All Saints' Preston on Tees.

1.3 Accountabilities

The PCC are deemed to be the responsible person or body for data protection purposes (i.e. act as joint Data Controller with the priest in charge of the parish). As such, the PCC are responsible for, and will demonstrate, compliance with the principles by:

- Adopting and implementing this data protection policy;
- Publish privacy notices to explain our data protection practices to those whose personal data we process
- Put in place written contracts with 3rd party Data Processors that process personal data on our behalf;
- Implementing annual reviews, to update the measures we have put in place
- Providing awareness and training appropriate to those processing personal data on behalf of All Saints' Preston on Tees

The PCC will appoint a Data Protection Officer who is responsible for assisting the PCC monitor internal compliance and to keep them informed and provide advice on data protection obligations (i.e. monitor data sharing agreements, data breaches, information risk, subject access requests and compliance with data protection policies and procedures). The contact details for the Data Protection Officer are published on the church web-site.

1.4 Definitions

- **Personal Data** - Any information that relates to an identifiable living individual. This covers both *personally identifiable information* (which is already in the public domain or has relatively low sensitivity such as names and addresses), and *sensitive personal information* that require additional care being taken when processing (e.g. race; ethnic origin; politics; religion; trade union membership; biometrics (where used for ID purposes); health; or sexual orientation. Sensitive personal information also includes personal bank account details, pay, medical information and personal data relating to safeguarding.

- **Data processing** – Any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.

- **Data Protection Impact Assessment (DPIA)** - A process designed to help systematically analyse, identify and minimise the data protection risks of a project or activity.

- **Data Subject** - The individual to whom the data being processed relates.

- **Data Controller** - A body or organisation that makes decisions on how personal data is being handled.

- **Data breach** - any occasion when personal data is: accidentally or unlawfully lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or made unavailable (through being hacked or by accidental loss/destruction.

- **3rd Party Data Processors** – Other legal entities that process data on behalf of a Data Controller and under instruction from the Data Controller. Data Processors do not have the ability to make decisions about how the data should be processed, there should be documented instructions from the Data Controller about what the processor can and cannot do with the data (known as a Data Processing/Sharing Agreement).

2 Principles of data protection

Personal data must be handled according to the following principles:

1. **Data is processed lawfully, fairly and in a transparent manner** in relation to the data subject, through the provision of clear and transparent privacy notices and responses to individual rights requests.

2. **Data is collected for specified, explicit and legitimate reasons** and not further processed for different reasons incompatible with these purposes, see Information Asset Register (Appendix 2) and Register of Processing Activities (Appendix 3).

3. **Data is adequate, relevant and not more than is necessary** to complete the task for which it was collected and will be subject to regular review of data collection and processing needs.

4. **Data is accurate and up-to-date** and reasonable steps will be taken to ensure this through regular data quality checks.

5. **Data is not kept for longer than is necessary** to complete the task for which it was collected (see section on record retention schedule). Data that is stored and used for archiving purposes

in the public interest, scientific or historical research or statistical purposes is the responsibility of the designated party owning that process.

6. **Data is kept secure**, with appropriate technical and organisational measures to protect against unauthorised or illegal processing, accidental corruption, loss or disclosure of personal data. This will include:
    - storing paper copies of personal data in locked cabinets;
    - maintaining password protection of electronic data held on computers and online storage;
        - ensuring access to paper and electronic media is restricted only to those individuals authorised to access the data;
    - ensuring that extra precautions are taken when personal data is carried in public places, to keep the risk of data breaches to an acceptable level.

    To maintain appropriate data security, we will undertake regular risk assessments of our practices.
7. **Data that is transferred outside the United Kingdom** will only take place with appropriate safeguards to protect the rights of individuals.
8. **Subject Access Requests (SAR).** Individuals have the right to request a copy of all information held about them with data storage areas managed by All Saints Preston-on-Tees.

3 Data management

3.1 Data Protection Impact Assessment

The PCC has adopted the principle of 'privacy by design'. All new projects, updated processes or significantly changed systems that require the use of personal data and may pose a high risk to data subjects, will be subject to a Data Protection Impact Assessment (DPIA). A DPIA template is available here: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04post-comms-review-20180308.pdf.

3.2 Collecting and handling personal data

Data protection legislation requires that the collection and use of personal data is fair and transparent. These requirements cover both personally identifiable information (e.g. information already in the public domain or address or other information that is low sensitivity), or personally sensitive information (e.g. bank account, pay, medical information or other personal details that are considered high sensitivity).

When using personal data, it is our policy not to write comments about any individual that are unfair, untrue or offensive and that you would not be able to defend if challenged. In general we:

- Express facts, not opinions
- Work on the basis that anything written about an individual might become public.

This includes the use of emails which although often information in nature are within scope of this policy if they contain personal information.

If we acquire any personal data related to an individual (including employees, officer holders, volunteers, suppliers, supporters or other external contacts), either directly from the data subject or from a third party, we must do so in line with the above 'Principles of Data Protection'.

If we acquire data in error (that is, data we should not have access to), by whatever means, we will immediately inform the Data Protection Officer who will assess how best to respond to the situation (e.g. record the incident, notify the individual and delete information).

3.3 Data Sharing

We recognise that when we share personal data with third parties, we are responsible for:

- ensuring the third party complies with GDPR, and
- stating any constraints or requirements about what the third party can or cannot do with our data.

When sharing or disclosing personal data we shall ensure that:

- We consider the benefits and risks, either to individuals or the Church, of sharing the data, along with the potential results of not sharing the data;
- We are clear about with whom we can share the data. If we are unsure, we check with the data owner, or our Data Protection Officer.
- We do not disclose personal data about an individual to an external organisation without first checking that we have a legitimate reason to do so (see above 'Lawful bases' section).
- If we must transfer or share data, we do so using appropriate security measures;
- If we are sharing data outside of the UK, we take particular care to ensure that the destination country meets all the necessary requirements to protect the data.

The above principles also apply to private donations which are made to the church. The size and origin of such donations will only be known by the Treasurer (or designee for a legitimate purpose such as an independent audit of church account) and will not be disclosed to other persons including clergy.

If we are unsure whether or not we can share information, we will contact the Data Protection Officer for our Diocese to provide help and advice.

Data Sharing Statements

We may state any constraints or requirements on the use of data shared with third parties in the following ways, depending on the level of risk:

- Through the use of disclaimer-type statements in emails or on contractor job sheets such as the following example.

> The attached personal data is provided by [name_of_data_controller] to [third_party_name] for the purposes of [state_the_purpose_here]. To comply with General Data Protection Regulation 2016/679 and the Data Protection Act 2018, this data is only to be used for [insert_name_here] to contact the persons listed in the attached data file for the above stated purpose. You must not share it with any other third party; you must store it securely and take all reasonable steps to prevent its unauthorised access, accidental deletion or corruption. When you no longer need this data, it must be deleted and any paper copies you have made destroyed. Should this data suffer an unauthorised disclosure (data breach), you are to notify [name and contract detail for lead data protection person].

- By the inclusion of a 'Data Protection' section of a contract with a third party (such as a leasing agreement)
- By a standalone 'Data Sharing Agreement'

3.4 Record Retention Schedule

The PCC refers to https://www.churchofengland.org/about/libraries-and-archives/recordsmanagement-guides and the "Keep or Bin – Care of church records guidance" for its record retention schedule. Data cleansing will be conducted annually as part of the PCC's annual review of this policy.

3.5 Storing and disposing of data

We will ensure that we use the most appropriate and secure methods available for both storage and disposal of personal data. We will ensure that:

- In so far as we are able, all personal data in our possession is kept secure from unauthorised access;
- We lock physical files containing personal data in a secure cabinet;
- We are vigilant of our surroundings, in particular when working outside of normal office locations, being careful not to place any personal data in a position where it can be viewed, stolen or lost;
- All devices used to handle personal data are password protected and we do not share passwords;
- Desks are kept clear of personal data when not occupied.

3.6 Data Breaches

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data . This includes breaches that are the result of unintentional or deliberate causes. It also includes where personal data is made unavailable, for example, if it is encrypted by ransomware.

Any data breach, as described above, is to be immediately reported to the Data Protection Officer.

Where a breach is known to have occurred which is likely to result in a high risk to the rights and freedoms of individuals, our Data Protection Officer will report this to the ICO within 72 hours and will co-operate with any subsequent investigation. We will contact the affected data subject(s) where it is necessary to do so.

3.7 Individual Rights

Data protection legislation gives individuals specific rights regarding their personal data that is collected or processed by All Saints, Preston-on-Tees:

1. The right to be informed – to be notified of processing of personal data and reason for this (see Privacy Notices below);
2. The right to access – to have a copy of personal data made available to the individual concerned (see Subject Access Request below);
3. The right to rectification – to clarify and correct personal records pertaining to the individual that is inaccurate or out-of-date;
4. The right to erasure - to request personal data is erased where it is no longer necessary for the PCC to retain such data;
5. The right to restrict processing – to withdraw consent for data processing of personal data at any time;
6. The right to data portability – to request that the Data Controller provide personal data and to transmit that data directly to another Data Controller (when technically possible);
7. The right to object – to dispute the accuracy or processing of personal data, to request a restriction is placed on further processing
8. The right not to be subject to a decision based solely on automated data processing (e.g. decision-making and profiling);
9. The right to lodge a complaint with the Information Commissioner's Office.

Privacy Notices

Individuals have the right to be informed about the collection and use of their personal data. The lawful basis for different areas of our data processing is defined in [Appendix 1] of this policy and indicated in the relevant Privacy Notice.

A Privacy Notice covering our data processing activities relating to personal data is published on our parish website and we will inform individuals about the privacy notice at the time we collect or significantly amend their personal data.

Subject Access Requests (SAR)

We will provide copies of personal information held upon formal request received from the individual to which the information relates. PCC will be notified of SARs at their first meeting after receipt. We will make all reasonable endeavours to provide individuals with the requested information within 28 working days from the date that PCC are notified of the request. Personal information related to other individuals within that information will be redacted where appropriate before being provided as an authorised copy.

3.8 Training

Support and training will be provided to all those involved on behalf of All Saints Preston-on-Tees in the safe and lawful processing of personal data.

APPENDIX

1 – Lawful bases (based on GDPR Article 6)

Personal data must only be processed once we have identified an appropriate lawful reason to do so. No single basis is 'better' or more important than the others, we must decide which basis is most appropriate depending on our purpose and relationship with the individual.

Legitimate interest (including vital safety interests)

The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Processing Safeguarding data will usually be considered as being included under this heading.

The Data Protection Act allows all organisations to process data for safeguarding purposes lawfully and without consent where necessary for the purposes of:

- protecting an individual from neglect or physical and emotional harm; or
- protecting the physical, mental or emotional wellbeing of an individual.

However, this only applies to the extent that complying with these provisions would be likely to *prejudice* the proper discharge of your functions. If you can comply with these provisions and discharge your functions as normal, you must do so.

Legitimate Interest Assessment. When can you rely on legitimate interests?

- When processing is not required by law but is of benefit to you
- When there is a limited privacy impact on the data subject
- When the data subject would reasonably expect your processing to take place

In order to use legitimate interests as your lawful basis for processing, your processing must therefore meet all of the following criteria:

- Have a specific purpose with a defined benefit
- Be necessary – if your defined benefit can be achieved without processing personal data then legitimate interests is not appropriate
- Be balanced against, and not override, the interests, rights and freedoms of data subjects

Legal obligation (including public tasks with clear basis in law)

Data processing necessary to comply with the law or processing that has a clear basis in law. This excludes contractual obligations but includes items such as processing safeguarding records and maintaining diocese records for baptisms/weddings/funerals.

Consent

The individual has given clear consent for you to process their personal data for a specific purpose.
Such consent must be valid (freely given, unambiguous, actively selected, can easily be withdrawn); Both giving and withdrawing consent must be recorded. Furthermore for consent to be valid, it must be a choice - so if the data subject refuses to give consent, does that mean that the service can't be provided? If it is an essential service (e.g. pension, payroll etc) then the Data Controller cannot refuse the service, so there is effectively no choice, so consent is not valid.

2 - Information Asset Register

This appendix lists the main areas of personal information collected and processed by or on behalf of All Saints Church Preston-on-Tees that require particular attention from a data security perspective. The list includes data processing activities that are relatively infrequent but potentially highly sensitive and therefore carries a high risk.

No.	Information asset and description	Storage: location and format	Sensitivity of data (DPIA risk)
1	Safeguarding Reports (allegations and investigations of named individuals with identified witnesses)	Safeguarding Reports and data concerning previous offences held on G Drive	High
		Personal emails held by clergy and PCC Safeguarding Officer.	High
2	Confidential Pastoral information (records that include sensitive personal information)	Paper notebook held by Pastoral Team Leader and Funeral Minister	High
		Personal emails held by clergy and Pastoral Team Leader	High
3	Payroll information (names/salary/pension)	HMRC payroll web account	High
		Spreadsheets held by Payroll Manager	High
		Bank web account	High
4	Bank Transfers (bank references/amounts for payments inc. standing orders made by and to individuals and groups)	Parish Giving Scheme (PGS) web account	Medium
		Bank web account	Medium
5	Gift Aid Information (names, addresses, amounts)	Gift Aid web account	Medium
		Paper declaration in file held by Gift Aid Secretary	Medium
6	Non-Confidential Pastoral information (records that include personally identifiable information)	Personal emails held by clergy, Pastoral Team Leader and Funeral Minister	Low to Medium (depending on nature of information)
7	Churchsuite (names, addresses, emails, mobile phones, ages of children)	Churchsuite web account	Low
8	Electoral roll (names, addresses)	Church spreadsheet held on G Drive	Low

A written assessment is needed for each high and medium risk information asset identified Appendix 2.

3 – Register of Processing Activities

Data Processing Activity

1. Reason/purpose: What are you trying to do & why?
2. Data Categories: What kind of data is involved. Is it personal identifiable information (e.g. information already in the public domain or address or other information that is low impact), or personally sensitive information (e.g. bank account, pay, medical information or other personal details that are considered high impact)?
3. Collection Point: Where does the data come from?
4. Processing Justification: What are you doing with this data, and why, including the lawful basis for processing
5. Database, Location & Access: What, where, who can access & how maintained. Secure?
6. Data Sharing: which, if any, other organisations (legal entities) do you share this data with?
7. Retention: How long do you keep the data and how is it deleted/destroyed?