Data Protection Procedures and Breach Management Procedures Policy For St Mary's Church, Almondsbury September 2018

1. Data Protection Policy Statement

During the course of our activities, St Mary's Church collect, store and use **Personal Data** about the people with whom it interacts. This may include information about parishioners, volunteers, clergy, employees, contractors, suppliers and other third parties. This data is gathered in order to enable St Mary's church to comply with its statutory obligations and to achieve its charitable objects of advancing and maintaining the Anglican religion through the operation of its parishes and its other activities.

Everyone has rights with regard to how their **Personal Data** is handled by organisations. St Mary's Church is committed to ensuring that **Personal Data** is properly and securely managed in accordance with the General Data Protection Regulation as from May 2018 ("GDPR"), which enhances the Data Protection Act 1998 ("DPA"), and believes this is an important part of achieving trust and confidence between St Mary's Church and those with whom it interacts. St Mary's Church will make every effort to achieve best practice in relation to data protection and will regularly review its procedures to ensure they are adequate and up to date.

Any breach of this data protection policy will be taken seriously and may result in legal action being taken against St Mary's Church or the individual responsible for the breach.

2. Introduction

The Parochial Church Council (PCC) and the Incumbent of St Mary's Church have overall responsibility for compliance with data protection legislation. They are referred to as Data Controllers. The PCC Data Protection Lead, Liz Tierney, is responsible for ensuring day to day compliance with this policy and the relevant legislation.

The GDPR requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that individuals should be told what the purpose of using their personal data before it is used and consent to such use;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are used;
d) Accurate and, where necessary, kept up to data. Personal data that is found to be inaccurate should be deleted or corrected without delay. All personal data should be periodically checked to make sure that it remains up to date and relevant;
e) Kept in a form which permits identification or data subjects for no longer than is necessary for the purposes for which the personal data are processed. For instance, records of pastoral care discussions should not be kept for a number of years without justification. Records could be kept, for instance, if all identification features were removed, referred to as 'anonymisation';
f) Kept securely. Pastoral Data storage should be safe and secure – in lockable filing cabinets or in password protected computer files. Names and addresses of individuals must not be left unattended.

This policy applies to all **Personal Data** created or stored by the Parish in whatever format (e.g. paper, electronic, film) and however it is stored (e.g. electronically or in filing cabinets).

All clergy, staff and volunteers of St Mary's Church who are involved in the **Processing** (which includes collecting, accessing, using and/or disclosing) of **Personal Data** held by St Mary's Church are **Data Processors** and have a duty to protect the data they process by complying with this policy.

3. General Statement

This policy is intended to ensure that **Personal Data** is dealt with in accordance with the data protection principles and with data protection legislation generally. St Mary's Church will therefore:

- Ensure that, when personal information is collected, the **Data Subject** is informed what data is being collected and for what legitimate purpose(s). The appropriate Data Consent form must be used – currently the following consent forms are available – General Data Consent, Cleaning Rota Data Consent form, Sides Rota Consent form, and Lich Gate Directory Consent form.
- Take steps to check the accuracy of data at the point of collection and at regular intervals thereafter – which should be every 5 years.
- Securely dispose of inaccurate or out-of-date data, or data which is no longer required for the purpose(s) for which it was collected. See Appendix 1 for data retention rules.
- Share information with others only when it is lawful to do so and inform individuals with whom their data may be and/or has been shared and for what purpose(s). The General Data Consent form allows us to pass information to the Diocese of Bristol provided the **Data Subject** has consented, but not to any other third party.
- Ensure that data is processed in line with **Data Subjects'** rights, which include the right to (more details can be found in Appendix 2):
    - To be informed;
    - To access (includes Subject Access Requests);
    - To rectification (correction);
    - To erasure (also known as the right to be forgotten);
    - To restrict processing;
    - To data portability;
    - To object;
    - Not to be subject to automated decision-making including profiling;
- Ensure that all clergy, volunteers and employees are aware of and understand St Mary's Church's data protection policies and procedures.

4. Data Security

St Mary's Church shall ensure that appropriate security measures are taken to prevent damage to or loss, theft, or unauthorised disclosure of **Personal Data**. In particular, all clergy, employees and volunteers shall take the following steps to secure personal information:

- Only those who are authorised will be able to access **Personal Data** and process it. Currently this is the Vicar, Parish Administrator and Data Protection Lead
- **Personal Data** will not be stored on individual PCs unless those PCs are protected by a password known only to authorised users, or stored on portable electronic devices or removable storage media unless those devices are password protected.
- Passwords will be kept confidential and will be changed regularly.
- PCs will be locked or logged off and paper documents will be securely locked away when individuals are away from their desks.
- Offices, desks and filing cabinets/cupboards will be kept locked if they hold **Personal Data** of any kind, whether on computer or on paper.
- When destroying **Personal Data**, paper documents will be securely shredded and electronic data will

be securely deleted.

- **Personal Data** removed from an office will be subject to appropriate security measures, including the use of passwords/passcodes and encryption of portable electronic devices and must be stored securely (e.g. not left in the boot of a car).

When receiving telephone or email enquiries, employees and volunteers will be required to exercise caution before disclosing any **Personal Data** and will:

- Not give out **Personal Data** over the telephone unless they know or can verify the caller's identity and their entitlement to receive the information requested;
- Require callers to put their requests in writing so their identity and entitlement to receive the information may be verified;
- Ensure **Personal Data** is securely packaged and consider the most appropriate means by which the data should be sent (e.g. special delivery, courier or hand delivery);
- Refer to the Data Protection Lead for assistance in difficult situations.

Personal Data will only be transferred to a third-party such as a contractor or supplier if the Data Protection Lead is satisfied that the third party has in place adequate policies and procedures to ensure compliance with data protection legislation, and that the Data Subject has given specific consent to that third-party.

5. Subject Access Requests

Any individual has a right of access to the **Personal Data** which St Mary's Church holds about them. To be valid, a **Subject Access Request** from a **Data Subject** for the information St Mary's Church holds about them must be made in writing, and this includes requests made via email.

All **Subject Access Requests** will be dealt with by the Data Protection Lead. Clergy, employees or volunteers who receive a **Subject Access Request** must forward it to the Data Protection Lead immediately in order that such requests can be replied to 'promptly' and in any event no later than 1 calendar month from receipt of the request.

No fees can be charged for dealing with **Subject Access Requests**.

St Mary's Church cannot limit the number of **Subject Access Requests** made by a **Data Subject.** However, a refusal or a reasonable fee can be charged for requests that are manifestly unfounded, excessive or repetitive. If there is a refusal to a **Subject Access Request**, the **Data Subject** must be told why and they have the right to complain to the ICO or go to court.

6. Monitoring and Review

This policy will be reviewed every 12 months and may be subject to change.

7. Contacts

Any queries regarding this policy should be addressed to the Data Protection Lead.

Further advice and information can be obtained from the Information Commissioner's Office at

www.ico.org.uk

Glossary

Data Controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. For the purposes of this policy the PCC and the Incumbent are the data controllers of all personal data held and used by St Mary's Church.

Data Processor means any person who or organisation which processes personal data on behalf of a data controller including clergy, employees, volunteers and other third parties whose role involves accessing or otherwise using personal data held by St Mary's Church. Data processors have a duty to protect the information they process for and on behalf of St Mary's Church by following this data protection policies at all times.

Data Subjects include all living individuals about whom St Mary's Church holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data and the information that St Mary's Church holds about them.

Personal Data means data relating to a living individual who can be identified from that data or from that data and other information which is in, or is likely to come into, St Mary's Church's possession. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g. a performance appraisal). It can even include a simple email address. Mere mention of someone's name in a document does not necessarily constitute personal data, but personal details such as someone's contact details or salary would fall within the definition.

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive Personal data means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or any criminal proceedings involving that person. Sensitive personal data can only be processed under strict conditions and such processing will usually require the explicit consent of the data subject.

Data Protection Lead is responsible for data protection issues, including support and guidance for others, such as the PCC and the Incumbent.

Data Retention Rules

More Detailed information about retention periods can currently be found in the Record Management Guides located on the Church of England website at: - https://www.churchofengland.org/more/libraries-and-archives/records-management-guides and select 'Keep or Bin – The Care of Church Records' (Note document is currently date 2009)

Below is a table of the relevant key Documents and their retention Rules

Basic Record Description	**Keep in Parish**	**Final Action**
Church Services		
Baptism, marriage and confirmation registers	Arrange phased transfer to the Archives & Local History Service	Permanent (deposit)
Banns registers	Arrange phased transfer to the Archives & Local History Service	Permanent (deposit)
Service registers	Arrange phased transfer to the Archives & Local History Service	Permanent (deposit)
Baptism certificates counterfoils, marriage certificates counterfoils, copy burial and cremation certificates, application for baptism, banns and marriages	Last Entry + 2 years	Destroy
General Parish Administration		
The Incumbent and other ministers		
Institutions, admission, Licences	Current year + 6 years	Review for possible deposit
Correspondence concerning appointments	Last action + 5 years	Review/ Sample
Correspondence & other papers on routine admin	Current year + 3 years	Destroy
Copies of replies to questionnaires or important circulars	Current year + 5 years	Permanent (deposit)
PCCs, Church Wardens & other Parish Officers		
Minutes of meetings	Last action + 5 years	Permanent (deposit)
Electoral Rolls	Last complete review + 6 years	Review/ Sample
Parish Profiles on vacancy in benefice	Last action + 5 years	Permanent (deposit)
Visitation Papers	Last action + 5 years	Permanent (deposit)
Visitors' Book	Last entry + 3 years	Destroy
Routine Correspondence	Current year + 3 years	Destroy
Church Finances		
Planned Giving Schemes	Current year + 6	Destroy unless anonymised
Gift Aid Declarations	Keep as long as valid + 6 years	Destroy
Pastoral Care, Safeguarding, and Health & Safety		
Accident Reporting Sheets and Book – if relating to adults	Date of incident + 20 years	Destroy
Accident Reporting Sheets and Book – if relating to children	Date of when child became an adult + 20 years	Destroy
Clear DBS Certificate or disclosure of confirmation	Within 6 months of recruitment decision	Destroy

Basic Record Description	Keep in Parish	Final Action
Risk Assessment recommendations and management plan in the event of an unclear or blemished DBS disclosure	50 years after appointment ceases	Destroy
Records of other safeguarding adult/child protection incidents within the parish or within a family/ by an individual where the parish was the reporting body or involved in care or monitoring plans. That is any sex offender risk assessment and monitoring agreement	50 years after conclusion of the matter	Destroy
Records of any children's activities & registers, and related general safety risk assessments. Any communication from parents or other parties in relation to the above	50 years after activity ceases	Destroy
Personnel records relating to any lay employee not working with children and vulnerable adults	6 years after employment ceases	Destroy
Personnel records with contact with children and vulnerable adults, including all documentation concerning any allegations and investigations regardless of the findings	50 years after conclusion of the matter	Destroy
Other Parish Records		
Rota Duty Lists	Current year + 2 years	Destroy
Routine Correspondence	Current year + 6 years	Destroy
Lich Gate	Last action + 5 years	Permanent (deposit)
Parish Organisations – e.g. Choir, Bell ringers		
Minutes, Reports and accounts	Last action + 5 years	Permanent (deposit)
Membership Lists	Last action + 5 years	Destroy
Choir & Bell ringing Register	Current year + 3 years unless children are involved when 50 years after activity ceases	Destroy

Appendix 2 - Rights of the Individuals

The right to be informed

Data Subjects continue to the have the right to be given 'fair processing information' which is through the Data Privacy Notice. When personal data is collected, Data Subjects need to be informed of our identity, how we intend to use their information, explain the lawful basis for the processing of their data, our data retention periods, and that Data Subjects have the right to complain to the ICO if they think that there is a problem in the way their personal data is being dealt with.

The right to access

Data Subjects have the right to be given confirmation that their data is being processed, access to their personal data and supplementary information (i.e. information that is usually supplied in the Data Privacy Notice)

The right to rectification (correction)

Data Subjects have the right to have their personal data corrected (rectified), if it is inaccurate or incomplete. If the data has been given to third parties (provided the Data Subject has consented), we must tell those third parties of the correction. Data Subjects must be told about the third parties to whom the data has been given, after they have consented.

The right to erasure (also known as the right to be forgotten)

Data Subjects have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

This does not mean that a Data Subject can immediately request that their personal data id deleted. If the purposes for which the data was collected still exists, then the Data Subject will not be able to request for the deletion of that data, unless it was given by consent and they are withdrawing their consent. For instance, safeguarding information about an individual cannot be deleted if the retention is still necessary, reasonable and appropriate - e.g. to protect members of the public from significant harm. Another example is that some financial information, such as that relating to gift aid, cannot be deleted immediately due to financial auditing regulations. The personal data on the Electoral Roll can only be deleted in accordance with the Church Representation Rules, examples include, if someone writes stating that they no longer wish to be included on the roll, or a person no longer lives in the parish and no longer attends public worship there. Information in perish registers cannot be deleted under any circumstances.

The right to restrict processing

Data Subjects have the right to restrict processing of their personal data in certain circumstances (for instance if a person believes their personal data is inaccurate or they object to the processing). If processing is restricted, we can still store the data but cannot otherwise use the data.

The right to data portability

This is a new right under GDPR. Data Subjects have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT system to another. It only applies in certain circumstances and is highly unlikely to affect parishes.

The right to object

Data Subjects have the right to object to processing in certain circumstances – e.g. if a parish has relied on legitimate interest to process data without consent and the Data Subject is not happy with this they have the right to object to the parish processing their data.

The right not to be subject to automated decision-making including profiling

GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention. This is unlikely to affect parishes.