CONFIDENTIALITY & DATA PROTECTION POLICY AND PROCEDURE

1. Background

The General Data Protection Regulations (GDPR) 2018 extend the 1998 Data Protection Act (DPA) which itself extended the data protection requirements of the 1984 Data Protection Act.

The legislation requires organisations to protect and respect the rights and privacy of information held on individuals, whether electronically or in print copy. This policy deals only with information held on employees of the church.

Specifically, any individual on whom information is held has the right to:

- be informed of the information held on them (to enable fair processing procedures)
- access to this information if requested (called a 'subject access request')
- have the information corrected if the information held is incorrect?
- having the information removed unless there is a legal reason for holding or retaining the data
- restricting the processing of their information in some instances.
- asking for information to be transferred (called data portability) to another IT environment in a safe and secure way
- objecting to the information being held (if consent has been not obtained)

2. Policy

The XXX Church is committed to ensure that appropriate measures on holding personal information comply with the requirements of GDPR. Processes are kept simple and clear to ensure that personal information held on employees is processed fairly and lawfully and that individual's rights regarding access to their personal data are provided for.

Our policy is designed to:

- Identify what information should be kept by whom and for how long.
- Ensure that only the minimum data is collected and held necessary for the purpose for which it was collected.
- Ensure that those individuals who keep records are clear about how to do this securely; also they know their legal responsibilities.
- Ensure that everyone knows how they can access information held on them.

This policy should be read in conjunction with guidance given about data protection given under Safeguarding.

3. Scope

This policy applies only employees of the Church and covers every aspect of their recruitment, selection, appraisal, training as well as pay, benefit administration and general terms of employment

4. What is your personal data used for?

Personal information is held both manually and electronically to:

- Manage our employees
- Maintain accounts and records
- Carry out our legal requirements as a charity

5. Registration

[It may be necessary for the church to be registered with the Information Commissioner depending on what data is held. Please check with the Commission at https://www.gov.uk/data-protection-register-notify-ico-personal-data. A small annual fee is payable.

If so state....The XX Church is registered with the Information Commission number XXXXXXX. The annual renewal date is XXXX.

Or, if it not necessary state:

As a small charity it is not a requirement that we should be registered with the Information Commissioner.]

6. Responsibility

6.1 Overall responsibility: XXX (usually a Deacon) is responsible for personal information held as well as ensuring that everyone understands what personal information is held, what it is used for, that only data relevant for our charitable work is kept and that consent is obtained.

6.2 Others entrusted with personal data: Some other officials (state other deacons/Trustees) are responsible for ensuring that they are aware of what personal information is held, that is relevant for the service provided and they uphold the importance of holding it securely and processing this information in a fair and lawful way.

6.3 Individual employees: are responsible for updating any changes to information held on them (e.g. address etc).

7. Consent

Consent to hold personal information is obtained in different ways depending on the data required. Forms used will clearly state the reason and require written consent via a signature: for instance, an Application Form and other specific HR information forms. For those where a Disclosure & Barring Service (DBS) check is needed, consent will obtained be on a Self Disclosure Form.

8. Data Recording

8.1 Data held: personal information is classified as 'sensitive[1]' and 'non-sensitive' and protected against unauthorised access or processing; it is a requirement that it is accurate, up to date, not kept longer than necessary and only contains factual information. Particularly, before any sensitive data is obtained, written consent must be obtained and an individual informed of their rights.

Records can be held either electronically or manually or in both forms.

8.2 Type of data held: detailed records **c**over items relating to general employment on right to work, pay, occupational health, and appraisal and so on. We may ask for some sensitive data (example – ethnicity) at recruitment for legal compliance and good practice against discrimination. The content of records for those who are appointed to work for us range from basic details, such as name and address, through to performance, health and payroll information. Copies of documents provided to prove your right to work which is required by law (including your passport or other specified documents) will be retained and stored securely. Where a driving licence is required in order to drive for work purposes a copy will be retained securely for insurance purposes.

For payroll purposes salary and bank personal data is passed to the Treasurer. Payslips are handed direct to employees by the Treasurer as is P60 information. P45 information is mailed to employees who have left.

8.3 Where and how held

8.3.1 Manual: these records are kept in secure, lockable cabinets.

8.3.2 Electronic Records: some records may be stored electronically. These have restricted access and are password protected. Passwords must be changed regularly and contain both alpha & numeric characters and be at least 8 characters long. When mailing records either electronically or by post they must be marked "Private and Confidential" to ensure their confidentiality is maintained.

[1] Sensitive personal data includes information on race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

Any users of personal data on or off the premises (e.g. PC, SMART phone or laptop at work or home) must ensure that the data is secure. This means only appropriate people should have access to the data, and records should not be visible to unauthorised people. In reality this means ensuring PC's have an active screensaver with password and you do not give your password to anyone else.

8.4 Review and retention of records: those holding records must periodically review and destroy material held that is no longer required to be held on an individual. This applies to both manual and electronic records (e.g. data held on e-mails, in a personal folder and any USB's) it should be done securely and paper disposal should be carried out via shredding.

8.5 Privacy Policy: the Church's Privacy Policy for employees is given in the Appendix. It should be given to any employee who requests it.

8.6: Guidelines on retention

Document or data	**Statutory Retention Period**	**Our retention period**
Payroll records	6 years plus current year	6 years plus current year
Pension records	Not applicable	Retained permanently
HR records	Not applicable	6 years after leaving
Recruitment Forms	Not applicable	6 months after recruitment
DBS Clearance documents	Date of clearance + up to 6 months.	6 months then deleted
Accident Records	Not applicable	Retained permanently

9. Data Subject Rights

Anyone on whom data is held have a right to view information held regarding them individually if they wish. This is called a 'Subject Access Request' [SAR]. It can be submitted by email, letter or verbally. The data must be processed within 30 days of receipt.

Access procedures and checklists have been developed. The main points are:

- Requests from past or current employees must be made to XXXX [state]
- The identity of the person making the request must be verified to ensure that information is only given to the person entitled to it (e.g. an ex-employee him/herself).
- All requests will be acknowledged in writing within 3 working days of receipt and will be processed with 30 calendar days of the original request. A summary of the broad description of information held and

the reason it is held will be given when acknowledging receipt of the request.

Information will be able to be viewed on site at the Church. A hard copy of the personal information held can be given if requested, as part of the access to information process

10. Process for disclosures to external sources.

The Church has a responsibility to be cautious in giving out information held s to third parties.

With some requests, such as from HMRC or the DWP, the Church has a legal obligation to supply the information requested. With others, from employers asking for a reference, there is no obligation, although generally the Church will supply factual data on basic employment having previously obtained written consent [dates of employment and position held etc]. With other requests, such as from building societies, written permission from the individual employee will be sought before any disclosure is given.

Disclosure Guidelines:

- Formal requests for information must only be disclosed to authorised individuals.
- Only those within the Church designated to provide this formal information will do so.
- A record will be kept of any requests acceded to.
- Where practical, requests acceded to will always be in writing.

11. Legal Compliance

It is most important that everyone understands and follows the above policy and complies with our obligations on data protection. Any failure to comply with these guidelines or the principles of data protection legislation could result in an intrusion into someone's privacy with serious consequences.

The Information Commissioner could uphold a complaint against both the Church and the individual responsible for the data. The individual may be personally liable under data protection legislation and a breach could result in a criminal record and/or a fine. Individuals whose personal data is held may also sue for compensation for damage and any associated distress suffered as a result of any breach of data protection

Any breach of the Data Protection legislation, whether deliberate or through negligence, may lead to disciplinary action being taken.

Appendix: Employee Privacy Notice - Data Protection General Regulations

1. Your personal data – what is it?

This is personal data about you such as your name, address and other details. Keeping this information and processing it is governed by the General Data Protection Regulations (the "GDPR").

2. Who are we?

The Church [state] is/is not registered with the Information Commissioner. If registered 'Our registered number is XXXXX'.

3. Why do we need your information?

The Church will use your personal data for the following purposes to:

- Manage our employees
- Maintain accounts and records
- Carry out our legal requirements as a charity

4. How do we process your personal data?

We ask your permission to give us certain information about yourself and we keep it up to date, store it securely and eventually destroy it. The information you give us is stored either manually, or electorally or both. We do not collect anything unnecessarily or keep it for longer than is needed. We protect your personal data from loss, misuse, unauthorised access and disclosure and by ensure appropriate technical measures are in place to protect your personal data.

5. Sharing your personal data

We will only share your data any external agencies with your consent. We do not share personal information for marketing purposes with third parties.

6. How long do we keep your personal data?

Personal data processed will not be kept for longer that is necessary for that purpose or purposes. Details of how long specific information is held are available on request.

7. Your rights and your personal data as an employee

Through contacting XXXX as an employee you have the following rights (unless subject to an exemption under the GDPR) to

- request a copy of your personal data held by us.
- request that we correct any personal data if it is found to be inaccurate or out of date;
- right to request your personal data is erased where it is no longer necessary to retain such data;
- right to withdraw your consent at any time;
- right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- right to object to the processing of personal data where applicable.
- right to lodge a complaint with the Information Commissioners Office.

8. Further Information

If you would like further information about how we process and protect personal data please initially contact XXXXX at XXXX