Aspley Christ Church
with Christ at the centre

DATA PROTECTION POLICY

"Data Protection Legislation" or "Legislation"	means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), the General Data Protection Regulation (GDPR), any laws in the UK enacting the GDPR or preserving its effect in whole or part following the departure of the UK from the European Union and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, together with, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office.

Data Protection Legislation is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of Aspley Christ Church ("the Church"), the Church will collect, store and process personal data about our members, people who attend our services and activities, employees, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will help maintain confidence in the Church. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Legislation and with this policy. The post is held by Pam Coward, email address: pamela.coward@gmail.com

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third-party data and any recorded information including any recorded telephone conversations, emails or CCTV images.

Employees and others (including volunteers and trustees) who process data on behalf of the Church (referred to in this policy as 'Employees') should assume that whatever they do with personal data will be considered to constitute processing.

Employees should only process data:

- If they have consent to do so; or
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll; or
- the processing is **necessary for legitimate interests** pursued by Aspley Christ Church, unless these are overridden by the interests, rights and freedoms of the data subject.

If none of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Compliance with the Legislation

Employees who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. This includes the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly, lawfully and transparently
- be obtained for specified, explicit and legitimate purposes and used only for those purposes

- be adequate, relevant and limited to the minimum necessary for those purposes
- be accurate and kept up to date (every reasonable endeavour should be used to personal data that is not accurate is corrected or erased without delay)
- be processed in a manner that ensures its security (*see Information Security policy at Appendix 1).*
- not be kept for any longer than required for those purposes *see Retention policy at Appendix 2).*

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice) unless there is a legal exemption from doing so. We will keep records of any information shared with a third party including a record of any exemption which has been applied.

Employees should follow the Data Breach Procedure *(at Appendix 3)* if they think they have accidentally breached any provision of this Data Protection Policy.

Sensitive data

We will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health, and genetic information
- Sexual life
- Criminal offences

Sensitive data may be processed in the course of our legitimate activities, but may not be passed to any third party without the express consent of the data subject.

Monitoring the use of personal data

We are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- any Employees who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;
- Employees who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;

- All Employees must consider whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- Employees must follow the Breaches Procedure (*at Appendix 3)* should they become aware of any breach of this policy;
- Employees will keep clear records of our processing activities and of the decisions we make concerning personal data (including reasons for the decisions) to show how we comply with the Legislation;
- Spot checks may be carried out;
- An annual report on the level of compliance with or variance from good data protection practices will be produced by Pam Coward:
- Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences;
- We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

Handling personal data and data security

This will be managed in accordance with our Information Security Policy *(see Appendix 1)*.

The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. If personal data is collected directly from an individual, we will inform them in writing of their rights by providing them with a 'Privacy Notice' at the time the personal data is collected or as soon as possible afterwards.

In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects may also have a right of portability in respect of their personal data, and a right to be forgotten. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to Karen Pigott in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within **30 days** of receipt of a valid request (where permitted under the Legislation, we may take a further 30 days to respond but we will inform the individual of why this is necessary).

When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is

being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

Changes to this policy

We reserve the right to change this policy at any time, including as needed to comply with changes in law. Where appropriate we will notify data subjects of those changes by mail or email.

Policy adopted on 28 August 2021
(Date of Church Trustees/Elders meeting)

To be reviewed in 12 months' time.

Schedule – ICO Registration

Data Controller: Aspley Christ Church

Registration Number: ZB180038

Date Registered: 16 September 2021 - Registration Expires: 15 September 2022

APPENDIX 1 – Information Security Policy

APPENDIX 2 – Records Retention Policy

APPENDIX 3 – Data Breach Policy

APPENDIX 4 – Complaints process