BLENHEIM FREE CHURCH
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 Blenheim Free 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 David Fisher.

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 the 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 Records 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 the Data Protection Compliance Manager;
- 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 the Data Protection Compliance Manager 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.

Adoption of policy

Policy adopted on 24th May 2018
(Church Elders meeting)

To be reviewed in 12 months' time.

APPENDICES

APPENDIX 1 – Information Security Policy

APPENDIX 2 – Records Retention Policy

APPENDIX 3 – Data Breach Policy

APPENDIX 4 – Data Protection Complaints Process

APPENDIX 1 - Information Security Policy

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.
In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy.
'Church data' means any personal data processed by or on behalf of Blenheim Free Church.
Information security is the responsibility of every member of staff, trustee, office holder, church member and volunteer using Church data on but not limited to the Church information systems. This policy is the responsibility of David Fisher who will undertake supervision of the policy.
Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.
We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular:

- All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed.
- Manual records relating to church members or staff will be kept secure in locked cabinets. Access to such records will be restricted.
- Access to systems on which information is stored must be password protected with strong passwords and these should be changed at once if there is a risk they have been compromised. Passwords must not be disclosed to others.
- We will ensure that staff and members who handle personal data are adequately trained and monitored to ensure data is being kept secure.
- We will ensure that only those who need access will have access to data.
- We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out above in the Data Protection Policy), e.g. password protection for documents and encryption.
- Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors (who will be treated as data processors -see below).
- We will ensure that any data processor engaged to process data on our behalf (e.g. for payroll) will act under a written contract and will give appropriate undertakings as to the security of data.
- Appropriate software security measures will be implemented and kept up to date.
- We will ensure that if information has to be transported or transferred, this is done safely using encrypted devices or services.
- Where personal devices are used to store or process personal data, they must be subject to appropriate security.

All breaches of this policy must be reported to David Fisher.

This policy will be regularly reviewed and audited.

Appendix 2 - Records Retention Policy

Storage of Data and Records Statement

1. All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

2. Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.

3. Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose or destroyed.

4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

5. Any data file or record which contains personal data of any form can be considered as confidential in nature.

6. Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". All staff, trustees, volunteers and members of the Church are required to have regard to the Guidelines for Retention of Personal Data attached hereto.

7. Any data that is to be disposed must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to the Data Protection Compliance Manager who will undertake secure shredding.

8. Special care must be given to disposing of data stored in electronic media. Guidance will be given by the Church Trustees to any group which has stored personal data relating to its members on for example personal computers which are to be disposed of.

Guidelines for Retention of Personal Data

If you have any queries regarding retaining or disposing of data please contact the Data Protection Compliance Manager (this is not an exhaustive list).

Type of Data	Suggested Retention Period
Personnel files (including training records and notes of disciplinary and grievance hearings).	• 6 years from the end of employment
Application forms / interview notes	• Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file.
Information relating to children *NB. You may find it helpful to read the following article:* http://safeinchurch.org.uk/record-retention	• Check for accuracy once a year • Record that child was a member of the group – permanent • Secure destruction of personal data other than name and fact of membership – three years after ceasing to be a member

Church member information	• Check for accuracy once a year • Record that adult was a member – permanent • Secure destruction of personal data other than name and fact of membership – three years after ceasing to be a member
Church group member information	• Check for accuracy once a year • Record that adult was a member of group – permanent • Secure destruction of personal data other than name and fact of membership – three years after ceasing to be a member
Gift Aid claims, Income Tax and NI returns, including correspondence with tax office	• At least 6 years after the end of the financial year to which the records relate
Statutory Maternity Pay records and calculations	• As Above • (Statutory Maternity Pay (General) Regulations 1986)
Statutory Sick Pay records and calculations	• As Above • Statutory Sick Pay (General) Regulations 1982
Wages and salary records	• 6 years from the tax year in which generated
Accident books, and records and reports of accidents	• (for Adults) 3 years after the date of the last entry • (for children) three years after the child attains 18 years (RIDDOR 1985)
Health records	• 6 months from date of leaving employment • (Management of Health and Safety at Work Regulations)
Health records where reason for termination of employment is connected with health, including stress related illness	• 3 years from date of leaving employment • (Limitation period for personal injury) claims)
Student records, including academic achievements, and conduct	• At least 6 years from the date the student leaves in case of litigation for negligence

Appendix 3 – Data Breach Policy

Introduction
Blenheim Free Church ("we") hold and process personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

Purpose
This policy sets out the procedure to be followed to ensure a consistent and effective approach throughout the Church.

Scope
The policy relates to all personal data held by Blenheim Free Church, regardless of format. It applies to anyone who handles this personal data, including those working on behalf of the Church. The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach.

Types of breach
An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.
An incident includes but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

Reporting an incident
Any person using personal data on behalf of Blenheim Free Church is responsible for reporting data breach incidents immediately to the Data Protection Compliance Manager, David Fisher or in his absence the Pastor. The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

Containment and recovery
The Data Protection Compliance Manager will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

Investigation and risk assessment
An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. The Data Protection Compliance Manager will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.
The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use

- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

Notification
The Data Protection Compliance Manager will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. The Information Commissioner will be notified, if at all possible within 24 hours of the data breach, if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO is available on their website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
Where appropriate, we will notify the data subjects whose personal data has been affected by the incident; such a notification may include a description of how and when the breach occurred, and the nature of the data involved, and specific and clear advice on what they can do to protect themselves and what has already been done to mitigate the risks.
The Data Protection Compliance Manager will keep a record of all actions taken in respect of the breach.

Evaluation and response
Once the incident is contained, the Data Protection Compliance Manager will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

Appendix 4 – Data Protection Complaints Process

Blenheim Free Church ("we") take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact David Fisher without delay.

David Fisher can be contacted through the Church as follows:
Phone number 01628 776873
Email address enquiries@blenheimfreechurch.org.uk

We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Any complaint received by us must be referred to David Fisher who will arrange for an investigation as follows:

1. A record will be made of the details of the complaint.
2. Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure.
3. The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation.
4. At the conclusion of the investigation the Data Protection Compliance Manager will reflect on the circumstances and recommend any improvements to systems or procedures.