Broadstone Baptist Church

Serving Christ in the community

Broadstone Baptist Church GDPR Compliance Documentation

Index to Contents

Broadstone Baptist Church

Serving Christ in the community

Broadstone Baptist Church 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 the church.

Information security is the responsibility of every member of staff, church member and volunteer using Church data on but not limited to the Church information systems. This policy is the responsibility of Jon Taylor (Deacon & Church Secretary) 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 ensure information security by:

Ensuring appropriate software security measures are implemented and kept up to date;

Making sure that only those who need access have that access;

Not storing information where it can be accidentally exposed or lost;

Making sure that if information has to be transported it is done so safely using encrypted devices or services.

Access to systems on which information is stored must be password protected. Passwords must not be disclosed to others. If you have a suspicion that your password has been compromised you must change it.

You must ensure that any personally owned equipment which has been used to store or process Church data is disposed of securely. Software on personally owned devices must be kept up to date. Do not use unsecured wifi to process Church data.

All breaches of this policy must be reported to Jon Taylor (Deacon & Church Secretary)

This policy will be regularly reviewed and audited.

Policy adopted on Wednesday 2nd May 2018 at Church Trustees/Leaders meeting)

Broadstone Baptist Church was registered with the Information Commissioners Office on 25/4/2018 for Compliance with the General Data Protection Regulations – Registration Reference A8282566

This notice first posted Sunday 6th May 2018

Broadstone Baptist Church

Serving Christ in the community

Broadstone Baptist Church Privacy Notice

How we use your information

Your privacy is important to us. We are committed to safeguarding the privacy of your information.

Why are we collecting your data?

We collect personal data to provide appropriate pastoral care, to monitor and assess the quality of our services, to fulfil our purposes as a church and to comply with the law regarding data sharing. In legal terms this is called 'legitimate interests'. When it is required, we may also ask you for your consent to process your data. We do not share your information with others except as described in this notice.

The categories of information that we may collect, hold and share include:-

- Personal information (such as name, telephone number, address and email address)
- Characteristics (such as gender, ethnicity, language, nationality, country of birth)

Storing your data:-

We hold your data for varying lengths of time depending on the type of information in question but in doing so we always comply with Data Protection legislation. We will contact you annually to check that the information we are holding is accurate and that you agree to us holding it.

Who do we share your information with?

We will not share your information with third parties without your consent unless the law requires us to do so.

Requesting access to your personal data:-
Under Data Protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information please contact Jon Taylor (Deacon & Church Secretary)

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

For further information on how your information is used, how we maintain the security of your information and your rights to access information we hold on you please contact Jon Taylor (Deacon & Church Secretary)

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact:- Jon Taylor (Deacon & Church Secretary)

First Posted Sunday 6th May 2018

Broadstone Baptist Church

Serving Christ in the community

Broadstone Baptist Church 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.

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 groups 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 Lis Webb 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 Leadership team to any group which has stored personal data relating to its members on for example personal computers which are to be disposed of.

Policy adopted on 3rd May 2018 at Church Trustees/Leaders meeting

Broadstone Baptist Church was registered with the Information Commissioners Office on 25/4/2018 for Compliance with the General Data Protection Regulations – Registration Reference A8282566

Signed..... Pastor Tim Gamston

Guidelines for Retention of Personal Data

If you have any queries regarding retaining or disposing of data please contact Jon Taylor

Types 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	• 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 cease 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 cease 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 cease to be a member
Income Tax and NI returns, including correspondance 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

Broadstone Baptist Church

Serving Christ in the community

Broadstone Baptist Church Church Data Breach Policy

Introduction

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, a 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 Broadstone Baptist 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 Broadstone Baptist Church is responsible for reporting data breach incidents immediately to Jon Taylor (Deacon & Church Secretary) or in his or her absence Pastor Tim Gamston 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

Jon Taylor 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. Jon Taylor 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

Jon Taylor will decide with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner 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 www.ico.org.uk/media/1536/breach_reporting.pdf

Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks.

Jon Taylor will keep a record of all actions taken in respect of the breach.

Evaluation and response

Once the incident is contained, Jon Taylor 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.

Broadstone Baptist Church was registered with the Information Commissioners Office on 25/4/2018 for Compliance with the General Data Protection Regulations – Registration Reference A8282566

This notice was reviewed and agreed at the Deacons Meeting May 2nd 2018

Signed..... **Pastor Tim Gamston**

Broadstone Baptist Church

Serving Christ in the community

Broadstone Baptist Church Data Protection Complaints Process

We take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact Jon Taylor without delay. Jon can be contacted as follows:

Phone number: 0779 253642

Email address: jguytaylor@hotmail.com

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 Jon Taylor 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 Jon Taylor will reflect on the circumstances and recommend any improvements to systems or procedures.

Broadstone Baptist Church was registered with the Information Commissioners Office on 25/4/2018 for Compliance with the General Data Protection Regulations – Registration Reference A8282566

This notice was reviewed and agreed at the Deacons Meeting May 2nd 2018

Signed..... **Pastor Tim Gamston**

BROADSTONE BAPTIST CHURCH - DATA PROTECTION POLICY

"Data Protection Legislation"	means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, including, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office.

The Data Protection Legislation ("the 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 Broadstone Baptist Church, the Church Trustees will collect, store and process personal data about our members, people who attend our services and activities, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will 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 Jon Taylor (Deacon & Church Secretary)

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 who process data on behalf of the Church should assume that whatever they do with personal data will be considered to constitute processing. Individuals 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
- If neither of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Compliance with the Legislation

Employees and others who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly and lawfully
- be obtained for specified lawful purposes and used only for those purposes
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for any longer than required for those purposes
- be used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected)
- be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction
- not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.

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 evaluate 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;
- 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 [insert name]. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling personal data and data security

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. Manual records relating to church members or staff will be kept secure in locked cabinets. Access to such records will be restricted. Computer files should be password protected.

We will ensure that staff and members who handle personal data are adequately trained and monitored.

We will ensure that passwords and physical security measures are in place to guard against unauthorised disclosure.

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 below).

Security policies and procedures will be regularly monitored and reviewed to ensure data is being kept secure.

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.

All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed. Any agent employed to process data on our behalf will be bound to comply with this data protection policy by a written contract. Personal data stored on a laptop should be password protected.

The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. 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 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 [insert name] 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.

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.

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
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such should only be held if the explicit consent of each employee is obtained or if one of the other conditions for processing sensitive data is satisfied.

Changes to this policy

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.

Policy adopted on 3rd May 2018 at the Church Trustees/Leaders meeting)

`

Broadstone Baptist Church

Serving Christ in the community

GENERAL DATA PROTECTION REGULATIONS – INDIVIDUAL AUDIT FORM

Please answer as many questions as you can or put N/A if it's not relevant to you.

Name: .....

Do you consider that you possess church "data" of one kind or another at your home address? (Excluding the Prayer Partners booklet)		**YES**	**NO**
Very briefly please describe the nature of the data you hold. ie Members / Building Committee or Deacons Meeting Agenda's / Minutes, Monthly Financial Statements, Gift Aid Info. Etc etc ➡➡			
If you do have data do you share it with others or is it for your sole use?		**SOLE USE**	**SHARED**
Is that hard copies, computer files, or both?	**HARD COPY**	**COMPUTER**	**BOTH**
Do you maintain any e-mail (grouped) list of the church family (members & non-members)?		**YES**	**NO**
Do you process/retain any financial data in relation to individuals? This would be bank details of some kind.		**YES**	**NO**
Do you keep any "data" of any (external) persons who do not regularly attend our church?		**YES**	**NO**
Is that "external" data relating to people who have moved on, people/youth/minors attending groups or people attending our outreach events? Please specify ➡➡➡			
Do you take & store any photos at any church events?		**YES**	**NO**
Do you know the combination of the church safe kept in the Phase One Building?		**YES**	**NO**
Do you keep a list of church key holders?		**YES**	**NO**
Any comments you care to add?			

Signed ..... Date.....