# Data Protection Policy

This data protection policy regulates how the Hayling Island Baptist Church (HIBC) processes and stores information about its employees, officers, members, volunteers, visitors, and other individuals it may encounter during the normal course of its activities. In so doing, the Church must comply with the General Data Protection Regulations and the Data Protection Act 2018. This legislation controls the collection and use of data by the Church, and the safeguards required to protect all concerned.

## DEFINITIONS

**Controller** The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**DPA** Data Protection Act 2018**.** This is the Act that details the UK's implementation of the EU's GDPR. It therefore makes provision for the regulation of the processing of information relating to individuals. Under this Act, every individual has the right to find out what information the government and other organisations holds about them and what it is being used for. The 7 principles of this Act match those of the GDPR:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

**Data subject** The individual in relation to which HIBC is holding information; in our context this includes:

- employees (currently a minister)
- volunteers (including leadership, teachers, outreach coordinators, designated officers for safeguarding, data protection, etc.)

- members (those who have expressed a desire to be formally welcomed into membership and have gone through the process of doing so)
- visitors (those who attend the church and wish to be communicated with, but do not wish to become members; those who attend various church events and request further information or need to provide data for safety reasons)
- those supplying services to the church (individuals and businesses that assist with various church tasks, such as Independent Examinations)
- those who submit queries about the church and its activities, particularly via our website.

| | |
|---|---|
| **GDPR** | General Data Protection Regulations 2018 - Europe's data privacy and security law, which includes hundreds of pages of requirements from organizations around the world. It imposes obligations on any organization that collects data related to people in the EU. The UK's application of this is explained on the Information Commissioner's Office (ICO) website: ico.org.uk where it is helpfully broken down into definitions and categories. |
| **Personal data** | Information relating to identifiable individuals. |
| **Processing** | Any operation, or set of operations, which is performed on personal data, or on sets of personal data, whether by manually or by automated means, such as:<br>collection; structuring storage; retrieval; communication; research; reporting; disclosure by transmission, dissemination, or otherwise making available for communication, reporting, or ministry purposes; alignment or combination; restriction; or erasure. |

## DATA PROTECTION PRINCIPLES

As far as possible, HIBC strives to commit to the following in relation to the processing of personal data of its members and affiliates:

- the Church processes personal data lawfully, fairly and in a transparent manner;
- the Church collects personal data only for specified, explicit, and legitimate purposes as outlined in its Constitution;
- the Church processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of the processing;
- the Church keeps accurate personal data and takes all reasonable steps to ensure that inaccurate

personal data is rectified or deleted without delay. However, this requires that members keep the Church updated about any changes to their personal data;

- the Church retains personal data only for the period necessary for the processing, or until it is requested to be removed from its communications base by the individuals concerned;
- the Church adopts appropriate measures to make sure that personal data is secure and is protected against unauthorised or unlawful processing and from accidental loss, destruction, or damage.

**The Church, its employees, and other individuals who process, or use, any personal information must ensure that they always follow the principles outlined in this policy. Any failure to follow the policy can result in disciplinary proceedings.**

## OBLIGATIONS

If anyone has access to personal data held by the Church, they are required:

- to access only data that they have authority to access, and only for authorised purposes;
- not to disclose data (such as giving out a home telephone number of a member) except to individuals (whether inside or outside the Church) who have been given appropriate authorization by the individual whose data is concerned, or by the organization as recognized by the individual when they joined as a member;
- to keep data secure (for example by complying with rules on computer access, including password protection, and secure file storage and destruction);
- not to hold personal data, or devices containing or that can be used to access personal data, without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store other people's personal data on local drives or on personal devices whose information was obtained specifically for Church purposes; and
- not to store their own personal data on devices, such as laptops, which are owned by the Church and designated specifically for Church use.

Failure to observe these requirements may amount to a disciplinary offence which will be dealt with under the Church's disciplinary procedures.

Where external contractors assisting the Church, for example with maintenance on machines or audits, involves access to personal data stored on these machines, this activity must be supervised by a Church representative. It is the responsibility of that Church representative to ensure that data confidentiality is maintained at all times.

## MEMBER OBLIGATIONS

Members are advised on joining about the information that the Church will collect, use, and retain about them, and those to whom such information will be disclosed (details of which can be found in "Data Protection Notice – Church"). Members must ensure that all personal data provided to the Church is accurate and up to date. They must ensure that they notify the Church Secretary of any changes, for example of address. The Church cannot be held accountable for errors arising from changes about which it has not been informed.

## CHURCH LEADER OBLIGATIONS

Church leaders who encounter personal data through the Church for the purposes of ministry, member communications, research, reporting, or training, will be covered by this policy. In such cases, leaders must be notified about, and abide by, the relevant provisions of this policy.

## LAWFULNESS OF PROCESSING

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is the Church's policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described as

- Consent – unless it is necessary for a reason allowable in the GDPR, the Church will always obtain explicit consent from a data subject to collect and process their data. In cases of children below the age of 18, parental consent will be obtained. As previously highlighted on DP Notice document. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights about their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in plain language, and free of charge, for example on the HIBC website;
- Performance of a contract - where the personal data collected and processed are required to

fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. an event cannot proceed without an address to meet at;

- Legal obligation - if the personal data is required to be collected and processed to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.
- Vital interests of the data subject - in a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. The Church will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.
- Task carried out in the public interest - where the Church needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.
- Legitimate interests - if the processing of specific personal data is in the legitimate interests of the Church and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

**Processing special categories and criminal records data**

The Church will process special categories and criminal records data primarily where it is necessary to enable the Church to meet its legal obligations and to ensure adherence to health and safety legislation; vulnerable groups protection legislation; or for equal opportunities monitoring purposes.

"Special categories" data and "criminal records" data require higher levels of protection. We need to have further justification for collecting, storing, and processing these types of personal data. We may process special categories or criminal records data in the following circumstances:

- in limited circumstances, with the subject's explicit written consent;
- where the Church needs to carry out its legal obligations;
- where it is needed in the public interest, such as for equal opportunities monitoring, or in relation to safeguarding;
- where it is needed to assess an individual's volunteering capacity on health grounds.

Less commonly, the Church may process this type of data where it is needed in relation to legal

claims or where it is needed to protect anyone's vital interests and they are not capable of giving their consent, or where they have already made the information public.

## RIGHTS OF THE INDIVIDUAL

Data subjects have the right to:

- request access to their personal information;
- be informed of what personal information has been recorded about them
- request rectification of their personal information;
- request the erasure of their personal information;
- restrict the processing of their personal information;
- object to the processing of their personal information;
- data portability (sharing their data with individuals and institutions of their choosing, e.g. if they move to another church)
- be informed about processes involving automated decision-making and profiling

Each of these rights are supported by appropriate procedures within the Church's "Data Protection Notice" that allow the required action to be taken within the timescales stated in the GDPR.

## ACCURACY OF PERSONAL DATA

The Church will review personal data regularly to ensure that it is accurate, relevant, and up to date. To ensure the Church's files are accurate and up to date, and so that the Church is able to contact a subject, or, in the case of an emergency, another designated person, subjects must notify the Church as soon as possible of any change in their person al details (e.g., change of name, address, telephone number, etc).

## SECURITY OF PERSONAL DATA

The Church has put in measures to protect the security of personal data, such as internal policies,

procedures, and controls to ensure that personal data is not processed unlawfully, lost, or damaged. If anyone has access to personal data during their volunteering, they must also comply with this obligation. If anyone believes that they have lost any personal data in the course of their ministry activities, they must report this to the Church leadership immediately.

## DATA BREACHES

The Church will record all data breaches regardless of their effect.

If a breach of personal data that poses a risk to the rights and freedoms of individuals is discovered, the Church will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a considerable risk to the rights and freedoms of individuals, the leadership will tell affected individuals that there has been a breach and provide them with information about the consequences of the breach and the mitigation measures taken by the Church.

The Church will consult and follow the steps laid out at Personal data breaches: a guide | ICO

## CONTRACTS INVOLVING THE PROCESSING OF PERSONAL DATA

The Church will ensure that all relationships it enters that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

## PRIVACY BY DESIGN

The Church has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to consideration of privacy issues, including the completion of one or more data protection impact assessments. This policy requires staff to ensure that the Data Protection Policy be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The data protection impact assessment will include:

- consideration of how personal data will be processed and for what purposes;
- assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s);
- assessment of the risks to individuals in processing the personal data;
- consideration of controls necessary to address the identified risks and demonstrate compliance with legislation.

Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

## INTERNATIONAL TRANSFERS OF PERSONAL DATA

Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

## PUBLICATION OF CHURCH INFORMATION

Information that is already in the public domain is exempt from the GDPR. It is the Church's policy to make as much information public as possible, and the following information will be available to the public for inspection:

- names of Church trustees;
- a list of employees (excluding any internal telephone lists)
- photographs of key volunteers who lead ministries

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Church's Data Protection Officer.

## DELETION OF PERSONAL DATA

A member may resign their membership from the Church at any time. After it has processed such resignations, and provided that the former member has not requested to remain on any mailing lists, the Church shall delete personal data that it holds about that member as set out in the Data Protection Notice.

## SHARING DATA WITH THIRD PARTIES

As a membership organisation, the Church shares personal data of its members with other members of the Church and also, on occasion, with the Baptist Union. It will not share personal data of members for any other non-legal reasons without the consent of the relevant individuals.

## REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICE (ICO)

The ICO is the independent supervisory authority for data protection in the UK. Their mission is to uphold information rights for the public in the digital age. Legally the Church is bound to pay the data protection fee, which funds the ICO's work, and allows it to be listed on the ICO's register of fee payers, which is intended to show that the Church takes data protection seriously. It is understood that having registered under the Data Protection Act 1998, the Church will not need to pay any new data protection fees until its registration expires. The ICO have committed to informing HIBC in writing before this happens, reminding the Church of what needs to be done next.

Any breaches (actual or potential) of this Data Protection Policy, or of data protection law, by the Church or any of its members, should be reported immediately to the Data Protection Officer. Breaches shall be reported, if required, via the Data Protection Officer to the ICO and/or directly to the member(s) whose data is affected. Normally breaches will be reported after consultation with the Deaconate.

Further information on Data Protection legislation can be obtained on the ICO website: www.ico.org.uk

## ADDRESSING COMPLIANCE TO THE GDPR

The following actions are undertaken to ensure that the Church always complies with the accountability principle of the GDPR:

- the legal basis for processing personal data is clear and unambiguous;
- a Data Protection Officer is appointed with specific responsibility for data protection in the organisation
- all staff and volunteers involved in handling personal data understand their responsibilities for following good data protection practice;
- training in data protection is provided to all staff;
- rules regarding consent are followed;
- routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively;
- periodic reviews of procedures involving personal data are carried out;
- privacy by design is adopted for all new, or changed, systems and processes.

The following documentation of processing activities is recorded:

- organisation name and relevant details;
- purposes of the personal data processing;
- categories of individuals and personal data processed;
- categories of personal data recipients;
- agreements and mechanisms for transfers of personal data to other organisations (e.g. other churches) and affiliated organisations linked to ministries in other countries, including details of controls in place;
- personal data retention schedules (i.e. how long the data is retained and under what conditions);
- relevant technical and organisational controls in place.

The Church and its Trustees as a body corporate are the Data Controller under the Act, and are therefore ultimately responsible for implementation corporately. However, the Church appoints a Data Protection Officer, supported by the Trustees, to ensure that the above actions are reviewed

on a regular basis as part of the management process concerned with data protection. The Data Protection Officer undergoes training to ensure knowledge of data protection law and practices.

Information about confidentiality and data protection must be provided to all new members and visitors prior to them having access to the Church's network and any personal data.

This policy should be read in conjunction with other related policies as listed on the HIBC website.