Liberty Church Data Protection/ Information Security Policy

Introduction

The trustees of Liberty Church are committed to ensuring that all personal data, sensitive or otherwise, is stored and processed in compliance with the Data Protection Act and takes into account all available GDPR guidance. At the foot of this policy (Appendix A) is further information from the I.C.O. regarding this Act which came into force May 2018.The aim is to ensure that staff and personnel of Liberty Church do their best to serve the community and anyone linked to the community in some way. This policy is designed to provide guidance, as well as procedures for all personnel in processing data. Liberty Church is considered the 'data controller'. No Third-Party company is involved in processing and storing such data.

Why is Liberty Church Processing Data?

The purposes of processing personal data at Liberty Church are the following:

1. Communication

In the context of Liberty Church this involves communicating to and with those who are regularly associated with Liberty Church, and/or have been previously associated with Liberty Church. Communication means informing them of any information regarding activities, ministries, or anything else regarding the life of the church.

2. Pastoral Care

This involves using personal information about a data subject to ensure that, as a church, we are providing excellent pastoral care to all partners/members of the church. This involves things like pastoral notes to ensure personal sensitivity by staff when caring for an individual and monitoring connect group attendance.

3. Administration

This is all general administration in order to manage the activities of Liberty Church. This involves administration like team rotas, and monitoring Sunday attendance.

Following these general guidelines, below is some practical guidance on how we will fulfil these guidelines as a data controller to the best of our ability. This should provide guidelines for all Liberty Church personnel in processing any personal data.

Introduction to iKnowChurch

Current practice for Liberty Church data processing is to use a secure, encrypted, online database as above. Specifically designed for churches, we will ensure that all personal data on this system is held securely (through the technical security procedures and encryption provided by this database), and only accessed by the appropriate people.

Personal data should not be processed in any other way than electronically, unless absolutely necessary, and even then, all information should be kept as secure as possible.

For this purpose, all paper-based personal information will be kept to an absolute minimum, and destroyed securely as soon as possible. Completed membership/consent forms will be kept in a secure and locked filing cabinet in the Liberty Church office, as this is considered evidence of

‘explicit consent’, but this is only accessible to authorised members of staff. There may be occasions where paper copies of some personal information are necessary to be stored for a long period of time e.g., for safeguarding purposes.

The Reasons for Processing

All personnel must ensure that the reasons for processing any data whatsoever, is in line with the stated purposes.

In other words, any data processed must be clearly related to one of the three stated purposes of processing. Any Liberty Church personnel using any data must regularly ask themselves the question, 'What is the purpose for processing this information? Is it for communication purposes, pastoral care or administration?'

Liberty Church Personnel

Central to keeping information secure, is defining tightly who can have access to any personal information. The aim is three-fold:

- Firstly-to ensure that no-one who is unauthorised can access this information unlawfully.
- Secondly-to ensure that there are strict procedures in place to ensure that those who are authorised can only access the specific information they require for their stated purposes.
- Thirdly-to ensure that those who are authorised are appropriate to have such access, and have been fully trained. We will endeavour to ensure that there are clear responsibilities for specific use of the information.

iKnow Practical Guidelines

As such, using the iKnow system, we will endeavour to fulfil the following:

1. 'Permissions' will be utilised to ensure that appropriate access to information is given to the right people.
2. All personnel with access to any personal data will have full training before they use 'iKnow', regarding permissions, appropriate use, and how to keep information secure. They will also be made aware of the Data Protection policy.
3. Only members nominated by the Church Council will have full access to all data, and the ability to access and change 'permissions’
4. Liberty Church staff will have full access to all personal data for the purposes of communication. There also may be the need for them to have access to information for the purpose of pastoral care (in some circumstances) and administration (in many circumstances). The permissions for each individual will be decided in line with their role description, whether a paid employee or as a volunteer.
5. Connect Group Leaders will have access to personal information for those in their connect group, regarding necessary information for communication (i.e.: letting relevant members know about an upcoming activity), administration (i.e.: distributing notes) and some pastoral care (recording attendance and or any pastoral concerns for later use).
6. Team Leaders will have access to personal information for those in their team, regarding necessary information for communication (i.e.: letting relevant members know about an upcoming activity) and administration (i.e.: distributing notes, and or rotas).
7. Other personnel who will require access to such information will be few and far between, and in such an event, permissions will be looked at very carefully to ensure that they only have access to that which is absolutely necessary to fulfil their role in the life of the church.

8. The information collected and processed by any Liberty Church Personnel must only be for the purposes stated - no other information must be collected, and will be considered 'excessive'. This is particularly important when making any notes regarding pastoral care. Personnel must ask - 'Is it relevant and necessary to record this data?'
9. Liberty Church staff will take all reasonable steps to ensure information is up to date (in-line with the purposes) although it is noted that this is primarily the responsibility of the data subject considering the context of church life.
10. If an individual is no longer regularly linked with the life of the church, and this comes to the notice of Liberty Church staff, the following procedure should be put into place: on leaving, an individual's information will be deleted, as soon as is practicably possible unless they have been the subject of a safeguarding concern or are in the process of a safeguarding investigation in which case data may be stored indefinitely.

Understanding the use of names, profile pictures and telephone number being placed on What's App groups related to church activities which may be used for the purposes outlined in this policy.

If a member has agreed to disclose their mobile telephone number and have given the Administrators of specific What's App groups permission to add to the group, then this puts them at risk of people in that group who are not on their contact list, viewing and using without your permission.

Authorised administrators of all What's App Groups relating to Liberty Church will ensure persons are aware of that risk before including them in such a group.

APPENDIX A

1. The Data Protection Act according to www.gov.uk

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles.

They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Your rights
Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

2. Find out what data an organisation has about you
Write to an organisation to ask for a copy of the information they hold about you.

If it's a public organisation, write to their Data Protection Officer (DPO). Their details should be on the organisation's privacy notice.

If the organisation has no DPO, or you do not know who to write to, address your letter to the company secretary.

How long it should take
The organisation must give you a copy of the data they hold about you as soon as possible, and within 1 month at most. In certain circumstances, for example particularly complex or multiple requests, the organisation can take a further 2 months to provide data. In this case, they must tell you:

- within 1 month of your request
- why there's a delay

When information can be withheld
There are some situations when organisations are allowed to withhold information, for example if the information is about:

- the prevention, detection or investigation of a crime
- national security or the armed forces
- the assessment or collection of tax
- judicial or ministerial appointments

An organisation does not have to say why they're withholding information.

How much it costs
Requests for information are usually free. However, organisations can charge an administrative cost in some circumstances, for example if:

- you're asking for a large amount of information
- your request will take a lot of time and effort to process

3. Make a complaint
If you think your data has been misused or that the organisation holding it has not kept it secure, you should contact them and tell them.

If you're unhappy with their response or if you need any advice, you should contact the Information Commissioner's Office (ICO). **ICO** icocasework@ico.org.uk
Telephone: 0303 123 1113 Textphone: 01625 545860
Monday to Friday, 9am to 4:30pm

Information Commissioner's Office
Wycliffe House Water Lane
Wilmslow
Cheshire
SK9 5AF
You can also chat online with an advisor.

The ICO can investigate your claim and take action against anyone who's misused personal data.