

Kings Community Church

Data Protection Policy

Introduction

King's Community Church, Southampton (KCC) seeks to keep to the Principles of Data Protection, as set out in the Data Protection Act 1998. We aim to always keep to its principles in the way we collect and use information about people.

We consider the lawful and correct treatment of personal information as important because:

- It is the law and we as a church respect and aim to uphold the law
- It is part of our vision and values to always seek to act with integrity
- It is a vital aspect of our trustworthiness and we recognise that people trusting the church is vital to carrying out our purpose
- We recognise that we also have a pastoral responsibility towards people to protect their personal information so that it is not used by those who intend harm (eg identity theft, fraud, blackmail, coercion, actions by sexual predators.)

To this end, we commit to deal with personal information properly and securely however it is collected, recorded and used.

Purpose of this policy

The purpose of this policy is to ensure that all who collect and use personal data on behalf of KCC are clear about the purpose and principles of Data Protection and to provide a framework for KCC to put procedures in place which ensure Data Protection is implemented.

To whom this policy applies

This applies to all staff and trustees of KCC and also to those volunteers who are entrusted with collecting and/or using personal data on behalf of KCC or in the name of KCC. It also applies to KCC contractors, auditors, consultants and anyone we collaborate with or acts on our behalf and may need access to data. For the purpose of this policy this group of people will be called "KCC Data Processors."

Consequences of not keeping this policy

KCC will take action against any KCC Data Processors not keeping this policy. Breaking or failing to keep the law on Data Protection could result in legal action being taken against KCC or any of KCC Data Processors.

To ensure that all KCC Data Processors know their responsibilities and duties KCC will create a written contract for all KCC Data Processors which they will sign before they are allowed access to the ChurchSuite database.

What data (information) is covered by this policy

This policy is about personal data. Personal data is **information relating to living and identifiable individuals** (data subjects). It includes any information from which a person could be identified, including photographs. At KCC most data is about members, attenders and those who are associated with the church or its ministries/services. However, to be clear, this policy also applies to KCC employees, job candidates, those giving references for

applicants, individuals hiring our premises etc. If we record even just the name of an individual, or just their photograph that is personal data.

Non-personal data includes: company information related to our suppliers, contractors, customers (eg organisations who hire our premises).

Our purposes in processing personal data

Processing means obtaining, holding, using or disclosing such information, whether that information is stored digitally (eg computer, memory stick, CD) or on hard copy (eg paper.)

At KCC the main areas of data we process are

1) Names, contact information, age, gender, marital status/family group

These are for the following purposes:

- to keep a record of those who are currently in or associated with the church;
- to provide pastoral care and organise ministries for those within the church and in the wider community;
- to communicate with people about the church, its activities, beliefs and services.

2) Wider information

Where we care for vulnerable adults or children without their parent/carer present, we also collect:

- Parent/carer contact details (even when the parent or carer has no affiliation with KCC)
- Medical and other related information

This is so that we can provide appropriate care for those people and contact someone for them if they need that. Usually this is a condition of the service of caring for these people, and we inform them (or the parent/carers) that consent to process this data is not needed.

3) Photographs and video (Visual images)

There is a separate policy covering this area.

KCC means of processing data

We use ChurchSuite software to keep our database: under the GDPR law they are known as our "Data Processors". Currently their terms and conditions are legally compliant and satisfactory to KCC and they stand as a contract between KCC and ChurchSuite. This situation must be kept under review.

This is not our only way of processing data. We also process data in these ways:

- on paper – collected on paper forms which are kept for reference by those who need the information, or then transferred to computer
- on computer – collected, then recorded on computer
- via email – people email those in KCC

All these areas will be kept under review, aiming for ever higher standards.

Data Protection Principles

KCC will follow the Data Protection Principles outlined in UK law. In practice this means KCC will:

1. Collect information in GDPR compliant ways

- We will state who we are, the purpose of collecting the data and say on what legal basis we will collect and process it. We will also include the relevant privacy information in brief, and explain how to access to all privacy information, how to change their privacy options etc.

- Where we rely on consent as our basis for processing this will be fully compliant with GDPR requirements (fully informed, freely given, opt-in, specific and verifiable.)
- Where consent is not the basis for processing, we will inform the data subject of what basis we have for processing
- We will ensure those giving their data are informed of all relevant information to enable them to make an informed choice about how to proceed.

2. Collect only the data we need

KCC will only collect information which we need for the purpose for which it is being collected or in ways people would reasonably expect, given the information they were given when submitting their data.

3. Use it only for the purpose for which it was collected

Or in ways people would reasonably expect. If our use of the data changes beyond that, we will ensure that data subjects are informed and given opportunity to change their choices.

4. Keep data safe and away from any who are not authorised to see it

This is covered by a Data Security policy and/or guidelines, and Confidentiality Guidelines but briefly it includes:

- securing data from accidental loss and malicious attempts to access (or block access). This includes having good IT systems (hardware, software and staff/volunteer procedures) to secure electronic data and good security for paper records.
- Ensuring that, especially with sensitive data, there are safeguards to prevent access by staff and volunteers who have no need to know that information
- Ensuring we do nothing which results in the sharing of personal data with other organisations unless we have either informed the data subjects that we will do so when we collected their data (and that was included in their consent), or gain extra consent for such sharing.

5. Keep it only if it is still relevant, accurate and up to date

If we have collected information from parents at Toddler group, for example, we will usually delete that data when the parent stops attending unless they are involved in KCC in other ways. How this is done is given in a procedure covering data cleansing.

6. Ensure data subjects can exercise their data rights

Data subjects have the following rights:

- To be informed of what personal data we have relating to them (and/or their children under 18)*
- To have their data corrected
- To change their consent options (where there are consent options.)
- To have their data deleted (the right to be forgotten.)
- To have their data transferred to another data processor in electronic format (eg a csv file.)

KCC are committed to honouring these rights, and have procedures which give more detail on how we will carry that out. There are legal exceptions regarding what we share with a data subject/delete etc which will be covered in the relevant procedure documents.

7. Ensure personal data is not processed outside the EEA

KCC will not transfer personal data to a country outside the European Economic Area unless we can be sure that the standards of data protection are equivalent to the UK law. This applies to cloud servers as well as to any electronic or paper transfer to other countries. If we need to, for example, write a letter to an embassy to enable someone to get a visa, we must have written consent from the data subject to do this.

Data Protection Officer

KCC Elders and Trustees (or management appointed by them) will:

- appoint a Data Protection Officer (DPO) who will take day to day responsibility for implementation of data protection
- ensure the Data Protection Officer has the resources to carry out the responsibilities of the role
- oversee the Data Protection Officer.

The exact job description is a matter for the Elders and Trustees to agree, but in general their responsibility is as follows:

- Be aware of legal and moral responsibilities related to Data Protection
- Ensure (in consultation with line manager and where necessary Trustees) that he/she has the ongoing training and information needed to carry out their role
- **Ensure that other policies and/or procedures are established, communicated and implemented in the areas listed below and in other areas as the need arises**
- Ensure that all Data Protection policies are kept up to date and relevant.
- Ensure that all Data Protection policies are communicated effectively to the relevant people and that all relevant people in KCC receive training (including update and refresher training) which allows them to carry out their responsibilities for Data Protection. Also ensure training for new employees/volunteers and for those taking on new roles
- Ensure this policy and other related policies are implemented, including monitoring of compliance across the organisation, including all groups which are wholly or mainly run under the supervision of KCC
- Work with the person or people responsible for employees to ensure that Data Protection is included in the contractual obligations of paid employees and that serious breaches of data protection will result in disciplinary measures
- Keep a Data Management log giving brief details of such things as what information is stored and where, who is responsible for that information, when there are requests for new data to be collected, what is agreed about the procedures for such collection etc
- Ensure KCC registration with Information Commissioners Office is kept up to date and oversee that KCC is fully compliant with the current requirements of ICO
- Keep Trustees informed of Data Protection issues and inform them of any significant difficulties or breaches in the area of Data Protection

The DPO, reporting to the Elders and Trustees, will establish and update policies/ procedures / guidelines and oversee their implementation as required for:

- Processing of all personal data held by KCC including employee records
- Any special arrangements for processing sensitive data eg for children and vulnerable adults
- Responding to data access requests and withdrawal of consent for data storage
- Use of Technology, including laptops, portable data storage devices etc
- Visual images of people
- CCTV
- Any other relevant area which may arise in the future.

Other related policies

There are other KCC policies which are also part of Data Protection.

Currently these are:

- KCC CCTV policy
- KCC Visual Images policy
- DBS disclosure policy

There are also many procedures, processes and guidelines which are documented elsewhere.

REVIEW PERIOD: 2 YEARS	
REVIEW TO BE DONE BY: Data Protection Officer reporting to the Trustees	
Next review is due:	June 2020

THIS POLICY	DATE	Name given to the policy at this point
First approved by Trustees:	21/05/2018	Data Protection Policy KCC 2018