Data Protection Policy

Including Data Retention and Information Security

General policy statement

The King's Church, Wisbech is committed to respecting the privacy of individuals and ensuring the personal information that has been entrusted to us is processed in accordance with the Data Protection Act (DPA) 1998 and General Data Protection Legislation (GDPR) 2018.

We will never share a Data Subject's information with others without their consent, unless legally required to do so.

Definitions used in this policy

Data Subject: the individual whose data we hold or use (eg. A church member, someone who has attended a course or event, someone who has filled in a card asking to be kept informed about the church and its events). A person becomes responsible for their own data at 13 years of age.
Data Controller: The King's Church, Wisbech (us).
Data Processor: this is any third party which process data on behalf of the Data Controller.
(eg. Hubb.Church website and church management platform (part of Endis Limited)).
Data Protection Lead: a named person within the church whose can be contacted with regard to any data protection matter and who is responsible for gathering and monitoring the relevant consent.

Privacy and Data Protection

1. How we collect personal information

1.1 We collect personal information directly from people:

- at church events when a registration form or 'Hello' card is filled out
- who sign up as a volunteer
- when they register or buy tickets for an event or course
- when they make a donation, or decide to use 'Gift Aid'

1.2 We collect personal information electronically when a person:

- registers for an account on our website www.kingswisbech.org.uk

- completes a digital 'Hello' card
- responds to an online survey or sign-up form
- registers or buy tickets for an event or course
- contacts us
- makes a donation, or decides to use 'Gift Aid'

2. What information we collect

2.1 The personal information we collect:

- Personal identifiers such as a person's title, name and date of birth (for those under 18).
- Contact details including postal address, postcode, email and telephone number.
- Financial information such as bank details (if making a donation or purchasing a ticket).
- Whether an individual is a UK taxpayer (for Gift Aid purposes).
- Attendance at various services, groups or events and courses (to aid with mutual care and follow-up).

3. Permissions

3.1 Special category data

Special category data includes things like race, trade union membership, or political affiliation, as well as religious belief.

As the information the church holds falls into the 'Special Category' this means we need to ask for explicit consent from Data Subjects (you) to store, share and use their data.

3.2 Children under 13

Explicit permission will be sought from parents or legal guardians of children under 13 years of age for their personal details to be held and processed on our bespoke church management software, Churchinsight.

When the child reaches 13 they themselves will be asked to give their own permission, as well as allowing us to keep holding the older data.

See our Safeguarding Procedure to see how we contact children.

3.1 Vulnerable Adults

If an adult at risk of abuse has a personal carer, Power of Attorney or next of kin, explicit permission will be sought from them for us to store, share and use their data.

4. Why we collect personal information

4.1 We collect personal information:

- For the smooth running and administration of our organisation.
- To keep a person informed about our church's events and activities.
- To keep volunteers informed of their tasks, training, rota reminders etc.
- To encourage people on their spiritual journey.
- To process donations.
- To reclaim tax on Gift Aid donations, if applicable.
- To fundraise more effectively.
- To provide a useful resource in the form of an online directory of users.
- To provide an interactive website where email is used to communicate with the users.
- To provide a security mechanism on our website whereby we can restrict content to certain groups of users.
- To help us to improve the service we offer.

4.2 Fundraising

Fundraising is essential for The King's Church, Wisbech to impact the town of Wisbech and to fulfil our mission to 'present everyone mature in Christ'.

We ask for donations, or 'tithes / offerings' and notify you when we are including this as part of our worship on a Sunday.

A 'donate now' button may be included in an e-newsletter.

4.3 Church emails

Our leadership team do not use their personal email addresses to make contact with individuals if we are contacting them on church business or within our role as a church leader. Contacting them with regard to any events or activities organised by the church will always come from an official church email account whose address ends in @kingswisbech.org.uk.

Church group emails are sent to mailing lists by using our website. Any replies are received in our official church email accounts as hosted by Hubb.Digital.

Church email sent to individuals are sent and received from our official church email accounts at Hubb.Digital.

If an email is sent from an individual's account to another individual this is not an official church communication and as such does not fall under our Data Protection Policy.

Individuals are asked to specifically join the different mailing lists with the exception of our youth and children's work, where parents are automatically signed up to the mailing list when they fill out a registration form.

5. Data Subject's rights and choices

GDPR gives Data Subjects the right to:
- Be informed as to how their data is going to be stored, used and secured through our Privacy Notice available at meetings.
- Request in writing and securely obtain copies of the personal information The King's Church, Wisbech holds about them which we will give to the Data Subject concerned within one month.
- Correct or update their personal information held by us at any time. This can be done by a Data Subject if they have login access to our website in the 'My Area' section. Or by contacting the church office and their data will be updated as soon as possible (within one month).
- Object to the use of their personal information for certain things (eg. Emailing you about a forthcoming course or event, but you may wish to still receive the emailed newsletter). Preferences will be updated once we receive a written request to do so and these will take effect as soon as possible (within one month).
- Request The King's Church, Wisbech to stop using their personal information at any time. Upon receipt of a written request we will delete all data held on a particular Data Subject as soon as possible (within one month) and all communication will stop at this time.
- Lodge a complaint with the Information Commissioner's Office about how we manage your data.

6. Church Directory

6.1 Online Address Book

Data Subjects will be given the choice to opt-in to sharing their personal information in the Church Online Address Book.

Everyone who explicitly opts-in to sharing their data via this format will also have access to everyone else's data who have also opted-in. A person will not have access to the online address book if they have not chosen to join it.

By logging in to 'My Area' of the church website the Data Subject can manage their contact details, make changes, update preferences and select which information you want visible in the address book or not. This can be done by the Data Subject at any time.

They also have the choice of being ex-directory where personal information is stored on the website/church management system to help with administration but will not be visible in the address book.

If a person leaves the church, their access to the website can be restricted so that they can no longer access the personal details of others.

7. Who we share your information with

We are absolutely committed to protecting your privacy. Our policy can be summarised in one sentence:

we will not share your information with others without your consent, unless legally required to do so.

7.1 Our data processors:

HMRC – If you are claiming Gift Aid, we are legally required to share your Gift Aid information with HMRC.

Endis Limited (of which Hubb.Church and Hubb.Digital are a part)) - This is the company we use to host our website and to run our church management software which includes our email mailing-lists. The same company also hosts our individual church email accounts.

8. Data Breach

A data breach occurs whenever the security of personal data is compromised. This could be as simple as sending an email to the wrong person, leaving a folder containing paper financial records on the bus, or wiping a computer drive which contained important records.

If a Data Breach is serious in that there is a high risk of an adverse effect against the Data Subject's rights and freedoms they will be notified of the breach within 72 hours.

If we experience a significant Data Breach we will notify the ICO within 72 hours and a record of the breach will be kept.

We will do everything possible to keep personal data safe and secure. Please refer to point 10 for our Information Security.

9. Data Retention

9.1 Financial Data

As a registered UK charity we have a legal obligation to disclose the financial information of a Data Subject who has chosen to add Gift Aid to their donation to HMRC.
As such the church is legally obliged to retain personal and financial information provided by a Data Subject until the close of the current tax year upon which the church Treasurer will make the Gift Aid application to HMRC.
If a Data Subject continues to attend the church their data will continue to be held and used for Gift Aid purposes in forthcoming years.
If a Data Subject has not been attending the church for 1 year from the date of their last contribution their personal and financial data will be destroyed after it has been submitted to HMRC at the close of that current tax year.

9.2 DBS Checks

We will retain DBS checks if the Data Subject to whom it refers is still actively working with children within one of our church ministries or until it expires. If it expires whilst the Data Subject is still working with children and vulnerable adults for our church we will get an updated copy.

If the Data Subject no longer works with children in one of our ministries or has left the church, we will destroy their DBS check within 1 year of their departure.

9.3 General Church Database and Paperwork

A Data Subject's personal information will be kept on the church database throughout the time that person is actively attending church, unless they activate their right to withdraw that information (see Data Subject's Rights below).

If a Data Subject does not come to church for 1 year their data will be deleted and destroyed and login access to the website will be revoked. This includes destroying all physical documents which contain their personal information.

To keep the information we hold current and up-to-date there will be a yearly review where current Data Subjects whose information is on our database will be reminded that we hold their data and to inform us of any changes. (See Data Update Procedure)

9.4 One-Off Events / Courses

A Data Subject who has signed up to attend a one-off event or course (something that is not run weekly or monthly) and is not a current church attender will have their personal details deleted and destroyed 1 month after the completion of the course / event (unless information is required to be held due to financial record keeping).

They will be given an opportunity to register interest in another forthcoming course or indeed be invited to join the general church database for regular attenders (if they start attending regularly).

10. Information Security

10.1 Physical Data

Paper based physical data (ie. forms, paper registers, response cards, letters etc) will be stored securely in a locked filing cabinet in the church office in the Octavia View Building in Wisbech. Prior to being brought to the church office it may be kept in the locked cupboard of the Queen Mary Centre which is privately hired by the church. The church office itself is locked and access is restricted to church group leaders and Ferry Project Staff, the key to the filing cabinet is to be kept in a key safe.

Any church business paperwork that includes 2 or more personal identifiers including application forms, attendance registers, response cards etc. will only be held securely at these locations and documents relating to the church finances which may be kept securely in a locked container at the home of the Treasurer. In exceptional circumstances, officers of the church may take physical data home, for the minimum length of time possible, to undertake work that cannot reasonably be conducted in the church office. They are then responsible for ensuring this physical data is kept in a locked container in their home and, once used, is destroyed using a shredder or brought to the church office to be stored long-term or shredded.

Any paper based data collected during a church activity or event at the Queen Mary Centre should be passed to the Administrator in the first instance, or to an Overseer or Deacon in the second instance, who will then take that documentation to the Church Office at Octavia View.

10.2 Electronic Data - Hard Drive

The church Hard Drive that contains personal data as well as other sensitive data is stored in the locked filing cabinet in the Church Office at the Octavia View building or in a locked cash box which is stored in the locked cupboard of the Queen Mary Centre which is privately hired by the church. The church office is kept locked and access is restricted.

The Treasurer has an encrypted hard drive which should be kept in the locked container for paper files, this USB stick contains personal data necessary for the completion of Gift Aid returns. No other personal information is stored on this hard drive and the information on it will not be used for any other purpose. Church officers who are required to download personal data to perform their duties should ensure that these documents are regularly deleted from their files and Recycle Bin.

10.3 Church Prayer Chain

The church hosts a Prayer Chain whereby someone may request prayers for themselves or others by contacting the church administrator who will send out the information via email to those signed-up to be part of the Prayer Chain. Only those who are actively involved within the church are able to be part of the Prayer Chain recipients but anyone may send in a prayer request.

Prayer requests should ideally be presented in writing, for example, via email but text or may be presented verbally. In the instance of a verbal request, this must be made directly to an Overseer or the Administrator. When the prayer request is given directly from the person who the information is pertaining to, all details given may be relayed via the Prayer Chain.

If a prayer request is given by an individual about someone other than themself the name will not be included to ensure anonymity and the circumstances will be kept general, specific details will not be provided.

10.4 Electronic Data - Website

Certain sections of our website, including the online Address Book and the Web Office, are only accessible by those with login permissions. This is coupled with specific access to certain groups or teams that an individual is involved in.

Web Office access is only granted to those who are church leaders or who are involved in administration and need the information and functions it provides (eg. Mailing channels). Again access is restricted only to the areas an individual needs.

The Secretary, Data Protection Lead, Webmaster and Overseers have access to the whole Web Office. Our website (which includes the Web office) is secure and encrypted with SSL encryption.

SSL Encryption - Their system is extremely secure and our site also has SSL encryption. You can manage your contact details on this system by logging in to your account on our website at any time.

Passwords - Passwords are encrypted and stored in the database via a 1-way salted hash. Secure password links are sent using time-sensitive, single use email authentication.

Multi-factor Authentication - Administrators have to set up multi-factor authentication for web office access. All of the Hubb.Church staff have multi-factor authentication forced for logging into the Hubb platform and management system.

Hosting & Backups - Hubb.Church servers are located in a secure data centre in London on a highly redundant virtualised platform. These servers are accessed via secure VPN by the technical team. Changes to data are backed up in bulk and sent to a secondary server in the same location every 5 minutes. Backups are also sent to a second data centre which is 100% independent of the first, every 5 minutes. Both data centres benefit from state of the art security and compliance.

Monitoring and Alerts – Hubb.Church has robust server monitoring and alerts sent to their staff who are on call 24/7, 365 days a year.

Security Scanning – Hubb.Church runs regular automated security scans on our servers (including the OWASP Top 10 list) and also periodically engage CREST certified penetration testers for manual testing. We are currently rated grade A and A+ on industry recognised security checking providers.

IP Blocking – Hubb.Church have continuous upstream DDoS mitigation, and our servers are constantly analysing incoming traffic using automated algorithms that automatically blacklist IP addresses originating any attacks on our servers. Our servers are kept up-to-date with all the latest security patches and only accept connections using the latest ciphers. Firewalls block all non-essential ports.

Credit Card Details - where payment systems are in use by an organisation Hubb.Church do not store credit card numbers; these are all handled by a secure third party payment processor so no such information could be accessed on our systems if there was ever a data breach.

Payment Processing - Card details are handed straight to a payment processing company who handles millions of payments every day and whose entire business depends on the security of the transactions they handle. No card details are seen, handled or stored by Hubb, or by the church.

Sensitive Data - All of the elements on the payment page which handle sensitive data such as card numbers are in iframes hosted by the processing company themselves and so are secured by their own secure certificate and not subject to any communication with our servers.

Personal Data - Personal details that are stored on the website can only be accessed by logging in using a unique user name and secure password. Full user details can only be accessed through the Web Office by those staff members who have been granted the required permissions. The website and web office are all fully encrypted with SSL encryption.

Permissions - Hubb gives us the ability to give granular permissions, so anyone who has access to our Hubb system can only see and edit what we would like them to.

10.5 Electronic Data – Email

Email Security - We use DMARC and DKIM to keep all emails secure.
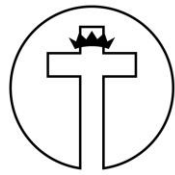
11. Our data protection lead

Please contact our Data Protection Lead with regard to any data protection matter.
Our Data Protection Lead is: **Verity McChlery**

Address: The King's Church, Wisbech
              10A-14 South Brink
              Wisbech
              PE13 1JQ
Phone: 01945 738030
Email: hello@kingswisbech.org.uk