Privacy Statement

Gateway Church is committed to protecting and respecting your privacy.

This statement explains when and why we collect personal information about people who visit us, our website, or connect with us on social media, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We may change this statement from time to time and a fuller version of our data protection policy can be found below. Both this statement and our policy are kept under regular review, so please check this page occasionally to ensure that you're happy with any changes. By using our website, or connecting with us on any other available touchpoint you're agreeing to be bound by this statement and our data protection policy.

Any questions regarding this Policy and our privacy practices should be sent by email to Richard Stamp at info@gatewaychurch.me or by writing to 133 Alder Road, Poole, BH12 4AA. Alternatively, you can telephone 0800 169 87 87.

Who are we?

We're Gateway Church Poole, a registered charity (no. 1135330) and company limited by guarantee (no. 7189544). Gateway Church is a member of the Evangelical Alliance. We are also a partner church of Advance, a global movement of churches aimed at planting and strengthening churches. More information about Advance can be found at www.advancemovement.com

How do we collect information from you?

We obtain information about you when you use our website, sign up for any of our events or groups on ChurchSuite, register a child with us for a kids group, fill in a Connect Card, apply to serve the church,

or a for a paid position, or make a donation using a gift aid envelope.

What type of information is collected from you?

The personal information we collect might include your name, address, email address, phone number, attendance information at events, groups and meetings, IP address, and information regarding what pages are accessed and when. If you make a purchase from us, for example for the purpose of purchasing event tickets, your card information is not held by us, it is collected by our third party payment processors, who specialise in the secure online capture and processing of credit/debit card transactions, as explained below.

How is your information used?

We may use your information to:

- Process a donation that you have made, and claim gift aid on it, with your written permission.
- Process transactions that you have requested, i.e. registering you for groups and events run by the church, or supplying you with tickets for events or products where that is applicable
- Ensure that any children attending a Gateway group or event are safely registered and accounted for.
- Send you communications which falls within the scope of the charitable objectives of the church, and for the purpose of developing a membership at Gateway Church Poole. This would be with your written permission, via our Connect Card
- Process an application for a job or a volunteer position

We review our retention periods for personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations (for example the collection of Gift Aid, or children's registration and attendance). We

will hold your personal information on our systems for as long as is necessary for the relevant activity.

Who has access to your information?

We will not sell your information to third parties.

Third Party Service Providers working on our behalf: We may pass your information to a third party associated organisation for the purposes of completing tasks and providing services to you on our behalf (for example to register you with an Advance event). However, when we use third party service providers, we disclose only the personal information that is necessary to deliver the service. Please be reassured that we will not release your information to third parties beyond the Gateway Church Poole and Advance Network, unless you have requested us to do so, or we are required to do so by law, for example, by a court order or for the purposes of prevention of fraud or other crime.

When you are using our secure online donation pages, your donation is processed by a third party payment processor, who specialises in the secure online capture and processing of credit/debit card transactions. If you have any questions regarding secure transactions, please contact us.

Your choices

You have a choice about whether or not you wish to receive information from us. We will collect your contact information via our Connect Card, and store it on ChurchSuite from where we send you details of church life, events and groups. If you do not want to receive these communications, you have the right to remove your information from ChurchSuite (you will be given a user name and password to be able to do this yourself), or you can request such a preference via the church office at any time.

How you can access and update your information

Gateway Church uses ChurchSuite to host and process all personal information of guests and members of the church, upon receipt of a completed Connect Card. Members are invited to download and access ChurchSuite for the purpose of staying in contact with the rest of the church and for adapting their communication preferences.

Alternatively, you can contact the church office at info@gatewaychurch.me or by post at 133 Alder Road, poole, BH12 4AA at any time with such a request.

You have the right to ask for a copy of the information Gateway Church Poole holds about you (we may charge £10 for information requests) to cover our costs in providing you with details of the information we hold about you.

Security precautions in place to protect the loss, misuse or alteration of your information

When you give us personal information, we take steps to ensure that it's treated securely.

Gateway uses Churchsuite as its data management system.
Churchsuite is a cloud hosted, web based management system which complies with the principles of the GDPR.
Below is a section of the ChurchSuite privacy policy:

"Maintaining the security of your data is one of our highest priorities, and to this end, all access to ChurchSuite is over an SSL (https://) connection, which provides 256-bit military grade encryption to ensure that all data in transit between your web browser and ChurchSuite is fully encrypted.

Where we are required to store any usernames or passwords for third-party integrations, such as social media or communication channels, we will always encrypt these details before they are stored on our servers.

Once we have received any data and stored it on our servers, we make commercially reasonable efforts to ensure its security on our system. To this end, we have chosen to host our ChurchSuite servers in a data centre that meets some of the strictest of industry security requirements, and is classified as a Tier 2 data centre.

Unfortunately, no data transmission over the Internet can be guaranteed to be 100% secure, so whilst we strive to protect your personal information, unfortunately we cannot warrant the security of any information you transmit to us."

This final paragraph applies to the transmission of data over the internet from any Gateway email account too.

Profiling

Using management information tools on ChurchSuite, we may analyse your personal information to create a profile of the various demographic groups within the church. We do this to ensure that the charitable objectives of the church are being met and that what we provide is relevant for all types of people.

Use of 'cookies'

Like many other websites, the Gateway Church website uses cookies. 'Cookies' are small pieces of information sent by an organisation to your computer and stored on your hard drive to allow that website to recognise you when you visit. They collect statistical data about your browsing actions and patterns and do not identify you as an individual. For example, we use cookies to store your country preference. This helps us to improve our website and deliver a better more personalised service.

It is possible to switch off cookies by setting your browser preferences. For more information on how to switch off cookies on

your computer, visit our full cookies policy. Turning cookies of may result in a loss of functionality when using our website.

For the purpose of keeping webstats and analysing how people interact with our website – for the purpose of improving it and making it fit for purpose, we may use software that allows us to track IP addresses and 'click' interaction with the website.

16 or Under

We are concerned to protect the privacy of children aged 16 or under. If you are aged 16 or under, please get your parent/guardian's permission beforehand whenever you provide us with personal information.

Review of this Policy

We keep this statement under regular review. This statement was last updated in April 2018.

Gateway Church Poole
Data Protection policy

Gateway Church Poole (GCP) is committed to following the principles of the UK Data Protection Act and to keeping the principles outlined in it. In particular, GCP seeks to ensure that the personal data it holds is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with an individual's rights to access, change the way it is processed, amend, alter or delete the data in line with the data subject's request
7. Kept securely

8. Subject to compliance with the principles of the General Data Protection Regulations (GDPR)

The GDPR applies to personal data stored in computer systems or structured filing systems, but the principles can be applied to all personal data that GCP holds in whatever form. The details of how these aims are achieved is worked out in the paragraphs below.

1) Registration

GCP considers that it is not exempt from registration under the General Data Protection Regulations, and aims to be compliant with it in full.

2) Gateway Church Poole's Legitimate Interests

Gateway Church Poole has a legitimate interest in collecting, processing and storing data for the purpose of developing a membership. The organisation presents its public benefit report in its annual accounts, and this public benefit is achieved through the development of a membership.

For example, when collecting Connect Cards from guests at our times of meeting, we will generally use that data to contact the giver of said data in order to assist them with any queries that they have about the organisation's business or to support them in line with our charitable objectives. Our charitable objectives are aligned with the development of a membership and so we consider there to be a direct and legitimate connection between collecting personal data and the achievement of our charitable objectives.

For reasons of clarity, our charitable objectives are summarised as follows:

a) To advance the Christian faith in accordance with our statement of beliefs in Poole at any place internationally
b) To relieve sickness and financial hardship and to promote and preserve good health by the provision of funds, goods or services of any kind, including through the provision of counselling and support in Poole or at any place internationally
c) To further Christian education including but not by way of limitation to children of pre-school age in Poole, or at any place internationally

d) To provide or assist in the provision of facilities in the interests of social welfare for recreation or other leisure-time occupation of individuals who have need of such facilities by reason of their youth, age, infirmity or disability, financial hardship or social circumstances with the object of improving their conditions of life in Poole or at any place internationally

Personal data is collected, processed and stored with these objectives in mind, as a legitimate interest.

3) Data Management

GCP uses Churchsuite as its data management system. For purposes of processing connect cards, registering for events, courses or groups, or registering children for children's work, we use churchsuite.

Churchsuite is a cloud hosted, web based management system which complies with the principles of the GDPR. According to the churchsuite privacy policy, data in transit between GCP and Churchsuite is fully encrypted, and stored in a Tier 2 data centre.

Churchsuite embodies the principles enshrined in GDPR since it puts the data subject in control of their data, giving them the right to amend data, make visible only the data that they wish to be made visible, and delete their data.

GCP churchsuite administrators who have access to every level of data held on churchsuite, are exclusively those who work in the office and are trained in data protection priniciples, and have read and understood this policy.

4) Data subjects

'Personal data' means information about a living individual who can be identified from that information and other information which is in, or likely to be in, GCP's possession.

With reference to point 2 above, GCP primarily holds personal data on:

a) Staff, including former members of staff and potential new staff, with their consent

b) Visitors including those who have identified that they wish to be considered as members of Gateway Church Poole, with their consent
c) Members of Gateway Church Poole, with their consent
d) Where applicable, and with consent, contact details for parents/guardians and carers of children who attend program events and clubs at Gateway Church Poole.
e) Others who have signed up for events, and groups at Gateway Church Poole, with their consent.
f) Anyone who donates to Gateway Church Poole and has signed a gift aid declaration
g) Anyone requiring a DBS certificate for work undertaken as a Gateway ministry

This list is not exhaustive – for example, GCP may also hold data on referees of those holding paid or voluntary roles within the organisation.

GCP also holds data on different supporting organisations, churches and trusts. Some of this data is not personal data – for example, the minister of a church is a matter of public record - and some data is effectively in the public domain but this does not necessarily reduce the responsibility to keep the requirements of the GDPR.

5) Good practice

a) Ensuring data is fairly and lawfully processed

Processing data has a wide meaning in the context of data protection and refers to any action involving personal information, including obtaining, adding, storing, viewing, copying, amending, extracting, deleting, disclosing or destroying information. GCP will ensure that the data it holds is processed fairly. The main test for this will be the subject's permission and expectation, i.e. will GCP staff and supporters feel this is a proper use of the information that is held?

In accordance with the GDPR, GCP will always endeavour to be explicit about this by explaining what use the information supplied will be put to. More information about this can be found on our Privacy Statement, which is published on our website. For the most

part, when collecting personal data, we will endeavour to communicate that:

- *We will use this information to keep you informed of GCP activities*
- *The information on this form/connect card/registration material will only be used to consider your application* (Application form for church membership/employment/voluntary position/CRB)
- *Your email and/or postal address will be used to send you information about church life, or to help us to establish or maintain church membership and will not be passed on to anyone outside GCP, except for the purpose of the above.*
- *Where data is used outside of the organisation, it will only be used for the purposes of the above, or within the wider context of church membership as expressed by the Advance partnership of churches to which we belong.*
- *Where this is the case, we will only ensure that your data is processed in countries that provide an adequate level of protection for your data or where the recipient provides appropriate safeguards, such as model contract causes, binding corporate rules, or mechanisms like the EU-US Privacy Shield framework.*

b) Ensuring data is processed for limited purposes, in line with an individual's rights and that the data held is adequate, relevant and not excessive

In order to be able to monitor and control what data is held and to meet the requirements of the GDPR, GCP encourages the holding of personal data within defined IT systems and databases. Currently these are:

- Churchsuite – see point 3 above
- Microsoft Office on shared drive - password protected for use by the Operations Manager, Administration Assistants, Treasurer and Elders.
- In a locked filing cabinet, offsite at the home of our Treasurer, for use by the Treasurer for the purpose of processing payments between the church and its members, and, for the processing of gift aid

Before designing sources for data capture, such as paper forms, response slips or web pages, the designer should review with staff each item captured to assess if it is relevant and how this information will be stored.

Personal data kept on a laptop then this data **must** be stored in a password protected document.

Personal contact data will not be passed to other organisations without the person's explicit permission or instruction.

Unless otherwise requested, Gateway intends to hold personal data for ex-members, and children who have participated in Gateway meetings or events, and records of any financial transactions, indefinitely for the purpose of safeguarding (especially for the purpose of retrospective investigation), and ensuring financial probity.

c) Ensuring data is accurate and up to date

Keeping data accurate and up to date is a difficult and ongoing task. GCP will make every effort to do this such as:

- Processing all returned mail to update records kept on churchsuite.
- Updating the records when advised of changes in direct debit instructions.
- Updating personnel records when advised of staff changes.
- Updating members personal details when advised of changes

Officers and members of staff in GCP are encouraged to regularly review the personal data they hold for accuracy and develop procedures in this area to ensure compliance

Use of the connect card is encouraged every Sunday, both for the collection of data, but also for any changes to any data that is held by the church.

In order to achieve this, a review of the data on churchsuite will be undertaken annually as part of the church's annual risk assessment.

d) Ensure data is not kept for longer than is necessary

GCP will continue to develop policies of securely destroying personal data when it is no longer needed. GCP currently destroy:

- Unsuccessful job/volunteer applications & references 3 months after the due date

- Applications for church membership when church membership ceases
- CRB disclosures as soon as a record is made of the disclosure number. In most cases this is immediate. We will however, keep an ongoing record of CRB numbers for safeguarding purposes.
- Successful job applications following the cessation of employment
- Personal information of guests (adult) within 12 months of consecutive non attendance at a Gateway Church Service or event (reviewed during annual risk assessment)
- Personal information of children (registration and attendance registers) after 6 years from last point of contact
- Gift aid envelopes after 6 years of cessation of an individual giving to the church

'Securely destroying' usually means the shredding of paper copies of data and the deletion of computer files, emails and database entries. When a computer is disposed of, computer hard drives **must** be cleaned with a "zero fill" secure deletion process or be physically destroyed before being removed from the building.

Officers and members of staff within GCP are encouraged to monitor the accumulation of personal data held and develop procedures in this area to ensure compliance.

e) Ensure data is kept securely

i) Physical security

The physical security of Gateway Church Poole & it's offices is an important part of keeping data secure. Because of the level of public use of the building, all personal data **must** be stored in the office which must be locked when not in use.

Staff **must** ensure that all paperwork containing personal data is removed from their desks at the end of a working day. It is recommended that sensitive records be kept separately in a locked drawer or filing cabinet.

In addition bank account details are treated as sensitive and these are only held by the Church Treasurer in hard copy in a locked filing cabinet.

It is essential that all sensitive hard-copy material is transferred hand-to-hand, or in the office safe, the code of which is known only to office staff, the treasurer and the church accountant. It should never be left in a folder in an unlocked place for a person to pick up when convenient.

ii) Network security

All personal data stored on a computer must be protected by a robust username and password for access. Passwords should be sufficiently complex and regularly changed. Staff **must not** share network usernames and passwords. Passwords for any computer system should not be written down on paper.

iii) Backups

Data is backed up for all staff via OneDrive

iv) Security of data in transit

When personal data needs to be transferred to other parties, care must be taken to ensure that the data cannot be accidentally disclosed to unauthorised recipients. Secure methods of data transfer need to considered in all cases - preferences should be given to methods that ensure the data is encrypted such as secure ftp or SSL connections.

If encrypted transfer is not possible, personal data must at least be password protected.

Email is not a secure way of transferring personal data, as potentially an email can be read at any intermediate server. If personal data is sent by email it is recommended that the files be password protected before being emailed.

USB data sticks represent a very high risk area for the security of data, because they are so easily lost. Personal data **must not** be stored on personal data sticks belonging to officers or members of staff.

Laptops also represent a high risk area. If personal data needs to be kept on a laptop then the laptop must be password protected for access by the owner only. Whilst laptops remain the property of the church, they have been assigned to staff and some volunteers for the purpose of the charitable objectives of the church. In this regard, responsibility for the security of the laptop and the data

therein remains the responsibility of the assigned user wherever reasonably possible.

v) Home and remote working

When working from home or other locations outside the office, staff **must** maintain appropriate levels of security, including physical security of printed material and data.

Special care should be taken in the transport of personal information to and from home. Physical data media containing personal information – paperwork and CDs – should preferably be kept in a locked briefcase and laptops should not be left unattended in public places.

vi) Guarding against disclosure

All staff should ensure that personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. Unauthorised disclosure may be a disciplinary matter, and may be considered gross misconduct in some cases. To guard against this, Churchsuite may be used

vii) Third Parties

Some third parties (Princecroft Willis) may on occasion obtain information pertaining to a Gateway Church Member for the purpose of auditing or payroll. These third parties are made aware of our Data Protection Policy as part of our condition of usage of said function, i.e. accounting and auditing.

viii) Breach of data

Immediately following any breach or loss of data, this should be reported to the Lead Elder and a nominated trustee. They shall determine whether said breach should be reported to the police. The decision for this should be based on whether the breach of data has resulted due to theft/fraud, or if there are any significant safeguarding issues to be considered as a result of the breach.

Any major breach of data will be reported to the Information Commissioners Office within 72 hours of the breach

As part of the annual risk assessment an assessment of the impact of data breach will be done and reported to the trustees.

6) Training

a) Staff

As part of the induction process, each member of staff will receive basic awareness training in the principles of GDPR and a copy of this document, as well as a copy of our privacy statement, and training to use churchsuite. This session will cover the principles outlined above and will also address particular issues that they may have within their job description.

b) Volunteers

Volunteers who work with personal data will be given a copy of this document, a copy of our privacy statement, training on churchsuite, and the ongoing opportunity to raise any questions or concerns related to the safe collection and processing of data.

7) Right to access information

Staff, supporters, and other data subjects have the right to access any personal data that is being kept about them by GCP either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request in writing to the church office. GCP aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the Trustees will explain the reason for the delay in writing to the data subject making the request.

Similarly, GCP recognises that all data subjects can at any time exercise their 'right to be forgotten'

Under certain circumstances, GCP may disclose personal information to the police and other law-enforcement bodies. GCP will do this only if it considers the request reasonable and proportionate.

8) Compliance

Compliance with the GDPR and with this policy is the responsibility of all members of staff and any volunteers who have been entrusted with personal data. Any deliberate or reckless breach of this policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with trustees in the first instance.

April 2018

Appendix A – Advice to Volunteers

Gateway Church Poole is committed to following the principles of the General Data Protection Regulations and to keeping the principles outlined in it. In particular, we seek to ensure that the personal data we hold is:

1) Fairly and lawfully processed
2) Processed for limited purposes
3) Adequate, relevant and not excessive
4) Accurate and up to date
5) Not kept for longer than is necessary
6) Processed in line with an individual's rights for access, amendment or deletion of their data.
7) Alterable in the way that it is used by us upon request of the data subject (the person who's data is in question)
8) Kept securely
9) Not transferred to other countries without adequate protection

The GDPR applies to personal data stored in computer systems or structured filing systems, but the principles can be applied to all personal data that we hold in whatever form. We work out the details of how we achieve these aims in our Data Protection policy.

As a volunteer working for, or serving Gateway Church Poole, you are required to follow the same procedures as staff in the handling and processing of data. If you are in doubt, please ask to see the entire data protection policy and ask for further advice.

The main issues that may arise will be:

1) Ensure data is kept securely

a) Please make sure that the data you have been given is kept securely, whether in paper or electronic form. If travelling by public transport, keep them within your other luggage as you travel so that there is no risk of items being left on a train, or similar.

b) USB data sticks are notoriously easy to lose. Please do not transfer personal data to these data sticks, unless they are encrypted.

c) When working from home, you **must** maintain appropriate levels of security, including physical security of printed material and data.

2) **Ensuring data is processed for limited purposes, in line with an individual's rights and that the data held is adequate, relevant and not excessive**

   Please ensure that the data you have been given is only used for the purpose intended and is not given to or shared with anyone else. The data must be destroyed/deleted once it is no longer needed for that purpose.