HOPE CHURCH, GRAVESEND: DATA PROTECTION AND PRIVACY POLICY

INTRODUCTION

"Your privacy is important to us at Hope Church": That is why we have written this "Data Protection and Privacy Policy", and we are seeking to put certain measures in place in the way the church is run that we believe will help safeguard your personal information. But why is this so important, and will it get in the way of church activities by introducing additional complexities?

We think it is important for several reasons:

1. Personal information about you remains your 'property', and as such, the Lord expects other people and organisations, (including the church), to take care of it and not mishandle it. Personal information is also valuable, and if misused or used for inappropriate purposes, it can result in personal embarrassment or loss to you. The warnings in the Bible against gossip, (e.g. Romans 1:29-30, Proverbs 20:19), are also very relevant: passing on information about people inappropriately is a serious sin. Looking after personal information well is part of our duty of care towards each person associated with the church, which we happily seek to meet.
2. On the other hand, being part of a church is something each of us does willingly and voluntarily, and it is natural that as we share our lives together within the church family, we will also need to share certain personal information with one another. This is inevitable if we are going to communicate with one another effectively, and pray and care for one another. (Note how the early church [Acts 2:44-45] were willing to share personal possessions with one another to meet needs). As we do so, it seems only sensible, (especially in our electronic age), to set out some basic guidelines about how best to protect one another's interests, while at the same time not introducing too many rules that might hinder our fellowship together.
3. Finally we do this because the government instructs us to. For many years there have been laws relating to this, but in May 2018 the law relating to data protection and privacy was enhanced in the UK by the General Data Protection Regulation (GDPR). This enhanced law gave extra rights and protection to the individual over the gathering and use of his or her personal data by organisations, including churches. So this Data Protection and Privacy Policy has also been written to comply with this law.

The nature of church life is such that there is an overlap between how we relate to one another as private individuals who are friends or family, and how we relate within the organisational structure of the church. In these guidelines we have sought to apply GDPR in a way that takes account of this, and is specific to how we serve one another in our activities at Hope Church.
We have also tried to be as inclusive as possible in producing guidelines that are easily understandable along with an Appendix providing a step-by-step guide for different roles within the church.

Philippians 2:4 "Each of you should look not only to your own interests, but also to the interests of others."

Terms Used in this Document

In the interests of clarity, transparency and inclusivity, we have attempted to make this Policy statement as understandable as possible by simplifying the language and terminology used as far as we can. It is necessary and appropriate, however, to introduce some terms that the law uses. We have listed and explained these below.

The essentials include:

General Data Protection Regulation: (or GDPR). This is the EU law which came into force in May 2018, and which will still be part of UK law following the departure of the UK from the European Union. It enhances existing laws from 1998 and 2003. It is designed to protect the interests and rights of individuals over their personal information, by seeking to ensure organisations, (including churches), handle that information fairly and lawfully, and that the privacy of individuals is respected. **In this document we will simply refer to the "GDPR"**.

Data Subject: Under GDPR a Data Subject is a living individual who can be identified from their personal data. In the context of this policy document, data subjects may include any individual with which Hope Church has dealings. This will include members of the congregation, members of the church, office holders, (whether paid and unpaid) and other employees of the church. It can also include individuals outside the congregation, encountered in the normal activities of the church, along with professional contractors or suppliers from whom the church receives services or advice. (GDPR does not cover data about companies or other organisations, but does include individuals within these bodies). **In this document we will simply refer to "individuals".**

Personal Data: This is personal information relating to a living individual. It can exist in a paper based or electronic format, and can include words or images. Personal data can be "factual", (e.g. name, address, date of birth, employment records), or an "opinion" about an individual, (e.g. notes on behaviour). **In this document we will refer to "personal data" or simply "data".**
We've included a statement in this document about the type of personal data we anticipate might need to be recorded.

Sensitive Data: This is data relating to specific facts or characteristics about an individual's race, ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, genetic information, sexual life and criminal offences. **In this document we will refer to "sensitive personal data" or "sensitive data".**

Processing: under GDPR this includes obtaining, holding, maintaining, storing, amending, erasing, blocking and destroying data, whether the data is held in physical or electronic format. **In this document we will refer to "processing", or identify clearly which specific part of the process is in view.**

Data Controller: under GDPR the Data Controller is the person or organisation that decides what data is processed, and that this is done for purposes that are legitimate, and in such a way that is fair and lawful. In the context of this document, Hope Church, Gravesend is the Data Controller. **In this policy document we will refer either to "the church" or "we".**

GDPR Principles: GDPR establishes certain principles that should be applied to the processing of personal data. **This document lists the 6 GDPR principles.**

Lawful Basis: under GDPR the church is required to have a good reason based on the law for processing personal data. As such we are accountable for and have to be transparent about our lawful basis for processing each type of data that we process. **This document will explain the different categories of 'lawful basis' under which we process individuals' data.**

Data Security: under GDPR individuals' data must be processed in a manner that ensures its security. **This document explains the measures that we intend to take to accomplish this.**

Data Retention: linked to the lawful basis for processing data is the requirement to retain data only for as long as necessary. We will only retain personal data for as long as required, and as long as we can do so under the law. It follows that the length of time we will retain data will vary depending on what that data is, why we need to keep it, and whether the law allows it to be kept. **This document will explain our data retention policy**.

Individual Rights: GDPR creates some new rights for individuals and strengthens some of the rights that already existed under previous laws. **This document will list these rights and explain and how we will seek to ensure these are safeguarded.**

Who is affected by this Policy

As already stated any individual that Hope Church has dealings with may come within the scope of this Policy.

It is possible to categorise the following groups:

1. **Individuals within the Church**
    - members of the congregation; a church congregation typically consists of people who attend the meetings of the church on a regular or occasional basis, some of them seeking to live out the Christian faith, others as enquirers into Christianity. Occasional visitors and passers-by that walk into a meeting may also come under this definition. Still others are present at the will of others, (such as the children of adults attending the meetings). Also included would be those unable to attend meetings regularly, (for instance due to ill health or infirmity), but who otherwise identify with the church.
    - church members as defined in our governing documents.
    - office holders; individual members are appointed to occupy specific leadership roles within the church. These may be paid or unpaid, such as pastor, elder, deacon, charity trustee.
    - volunteers with responsibilities within the church; though not necessarily office holders, examples may include treasurer, administrator, junior church and youth club leaders and helpers.
    - other employees of the church; such as cleaner or administrator;

2. **Individuals outside the Church**
    - this may include parents or legal guardians of children attending church or young people's meetings or other activities, where they are not personally in attendance;
    - visiting preachers and other speakers, and representatives of missionary organisations;
    - supporters of the church receiving news and other communications by email or by post;
    - professional contractors or suppliers from whom the church receives services or advice;
    - other members of the public encountered during the normal activities of the church.

Six GDPR Principles

Here we simply list the six principles under GDPR that should be applied to any collection or processing of personal data. Certain aspects of these are enlarged upon in the pages that follow.

Personal Data;

1. must be processed lawfully, fairly and transparently;
2. can only be collected for specified, explicit and legitimate purposes, and used only for those purposes;
3. must be adequate, relevant and limited to what is necessary for processing;
4. must be accurate and kept up to date;
5. must not be kept for any longer than is necessary for processing;
6. must be processed in a manner that ensures its security.

Lawful Basis for Processing Personal Data

GDPR lists six categories of Lawful Basis for processing personal data, as follows:

- **Consent** – an individual has given clear consent for their personal data to be processed for a specific purpose.
- **Contractual** – processing an individual's personal data is required to fulfil a contract, or because other specific actions are required before entering into a contract.
- **Legal Obligation** – personal data needs to be processed in order to comply with the law.
- **Vital Interests** – the processing is necessary to protect someone's life.
- **Public Task** – personal data needs to be processed to perform a task that is in the public interest.
- **Legitimate Interests** – it is in an organisation's and the individual's legitimate interests for the organisation to keep or use their personal data.

These six are not listed here in any particular order – no single basis is 'better' or more important than the others. Which basis is most appropriate to use will depend on the reason personal data is to be 'processed', and the type of relationship that exists with the individual. In practice some of these six are more relevant than others in the life of the church.

The most commonly used lawful basis for Hope Church to process your personal data is **legitimate interests**. As a church we exist for the mutual benefit of the individuals associated with the church and for the furtherance of our charitable and religious objectives, namely the advancement of the Christian faith. In order to do this, as part of the normal activities of the church, personal data about individuals will be voluntarily shared, recorded or acted upon. We of course recognise, (as does the law), that our legitimate interests cannot override the legitimate interests and rights of individuals.

In other cases the lawful basis is likely to be **contractual**, such as when individuals are acting on behalf of businesses providing a service to the church, or where an individual is contracted to work for the church.

Sometimes the activities of the church involve compliance with legal responsibilities in relation to government bodies, (such as with Safeguarding or Financial Accounting). In this case the lawful basis for processing personal data will be **legal obligation**.

Where none of these three common conditions apply, the church will need to establish a lawful basis by seeking individual **consent** if personal data is to be processed.

What Data is Processed?

What is not included under this Policy?

- **Sharing personal data privately within the congregation**: the nature of the church is like a family, and as such, members of the congregation may voluntarily share personal information between themselves and the church's Privacy Policy and Privacy Statement cannot make any commitments or statements about information shared in a private capacity.
- **Sharing personal data in public meetings**: information may be shared by individuals in public meetings, such as the Sunday services or the prayer meetings, which may include sensitive personal data, such as health. Since these meetings are public, and since non-members have access to them, they cannot be covered by the church's Privacy Policy or Privacy Statement. Although lying outside of the scope of this Policy there should be a general understanding and presumption that private information shared in a prayer meeting should be treated as confidential. However, individuals representing the church (e.g. leading a public meeting) should seek permission before sharing sensitive personal data.

What personal data and sensitive personal data is the church likely to process?

- We hold personal data about individuals employed by the church for the purposes of remuneration, taxation and where appropriate, pension provision. Individuals may be employed on a full-time or part-time basis, for example the pastor, or on an ad hoc basis such as the church cleaner or administrator. We may also share personal data about individuals employed by the church with Stewardship Ltd and HMRC. **Basis: legal obligation**
- We will maintain a list of the names of those who have joined the church as members. Contact details such as addresses, phone numbers and email addresses may be recorded for the purposes of internal communication, spiritual care and fellowship and the sharing of our lives with one another. **Basis: legitimate interests**
- We may also maintain an informal list of individuals attending the church on a regular basis, but who have not yet identified with us as members. This too will include contact details, and is for the purposes of communication and spiritual care. **Basis: legitimate interests**
- We hold contact details of officers of the church for the purposes of internal communication between individuals within the leadership of the church. This data is also for the purposes of providing contact details for other individuals and organisations corresponding with the church. **Basis: legitimate interests**
- Written notes may be taken and minutes produced in connection with member's meetings, and these may include elements or summaries of named individuals' comments and their contribution to the conversations in these meetings. **Basis: legitimate interests**
- Officers of the church may keep on record correspondence, (written or electronic), with individuals, (members of the church, the general congregation and others outside of the congregation), or notes taken at meetings. This is in the **legitimate interests** of the church in protecting the reputation of the church and its members and this information

may be kept indefinitely. These may not be destroyed or made anonymous as a result of an individual's 'request to be forgotten'. (An example might include a statement made in a church member's meeting revealing personal information, recorded within the minutes because it is pertinent to the matter being discussed, where it would render the minutes meaningless if the information were deleted. The purpose of minutes is to record the events and statements that were made at the meeting. Similarly this might apply to an email making a statement of fact needed at a later date to protect the reputation of the church or its members). **Basis: legitimate interests**.

- We may hold personal data about supporters of the church who do not form part of our regular congregation, but wish to receive news for their interest and prayers. **Basis: consent.**
- We may hold personal data about occasional visiting preachers and missionary organisation representatives. **Basis: legitimate interests.**
- We may hold personal data about individuals representing professional companies or other organisations that provide services to us. **Basis: contractual**
- We record donations from individuals who have entered into an arrangement with the church under the Gift Aid scheme. These may be made by standing order or cheque or as cash donations where the donor may be clearly identified. We share data with Association of Grace Baptist Churches (SE) and HMRC in order to process Gift Aid. **Basis: legal obligation.**
- Where expenses made on behalf of the church are reimbursed direct to personal bank accounts, bank details are recorded for administration and financial accounting purposes. **Basis: consent.**
- We hold personal data, (including potentially sensitive data), about individuals for whom we have arranged Disclosure and Barring Service checks. In addition we will record information about individuals in the course of monitoring safeguarding. In the event of a safeguarding incident we might then record further information which might be of a sensitive nature. **Basis: legal obligation**
- We share data with Association of Grace Baptist Churches (SE), DBS Disclosure Services Ltd and the Disclosure and Barring Service in order to carry out DBS checks on those involved with working with children and young people. **Basis: legal obligation**
- Under the church Safeguarding Policy, by consent, we will gather, record and retain personal data, (including sensitive data such as medical information), relating to children and young people under the age of 18 from their parents or legal guardians. In addition we will retain the names and contact details and signatures of next of kin or legal guardians of these children. **Basis: consent and legitimate interests**
- Photographs may be taken for church use, with the following arrangements, (some additional details are contained in the church Safeguarding Policy):
  - The church will have designated photographers, one of whom will take responsibility for collating photographs, deciding which to use, storing and backing them up securely.
  - Photographs may be used for publicity, (e.g. website, banners, leaflets), or in displays or photo books. Photographs will be for church use only and not for third party use, unless specific permission has been obtained, (e.g. newspaper report).
  - Permission for photographs will be taken in two stages.
    i. When an event is taking place and photographs are to be taken, an announcement will be made, so that individuals (including parents/carers on

behalf of their children) may opt out if they wish by telling a church leader or the photographer.

ii. If it is decided that a particular photograph is suitable for use in publicity material, then all those shown in the photograph will be asked to sign a form to confirm consent. **Basis: consent and legitimate interests**

- Photographs for personal use: as a church family we will meet on social occasions, and it is reasonable for people to take photos. These should, however, be for personal use only and should not be posted on any social media site, unless specific permission has been given from everyone in the image.
- Services are relayed via CCTV to other rooms in the chapel, with one camera focussed on the speaker at the front and a second camera located in the upstairs room. Our services are not broadcast live on the internet, and images are not recorded. Only audio recordings of our services are posted on the internet. If this situation changes in any way, we will review this Policy immediately. **Basis: legitimate interests**
- Under the Safeguarding Policy, in certain circumstances, it may become necessary to share personal and sensitive personal data with statutory bodies such as social services or police. No personal or sensitive data will ever be passed to any third party without the express consent of the individual, unless required by law to do so. **Basis: legal obligation**
- As part of the regular work of the church, we may engage in neighbourhood visiting, where we seek to make contact with members of the local community. When this is undertaken, we will keep a record of addresses visited to avoid duplication, and also where individuals have been encountered, we may also record brief notes where appropriate about conversations that have taken place, to serve as an aide memoire for prayer and to facilitate follow up visits. These notes may include sensitive data such as religious beliefs. **Basis: legitimate interests**

Data Rights

The GDPR creates certain rights to individuals in relation to their personal data.

1. **The right to be informed if your data is being used:** you have the right to be told how and why we are using your personal data, how it will be stored, and for how long, along with your other rights under GDPR. This is called 'privacy information', and this explanation is called a 'Privacy Notice'.
2. **The right to get copies of your data:** you may exercise your right to access your personal data by asking for a copy of the data. This is in order to check what data is held and to ensure it is being handled lawfully. This is known as making a 'subject access request'.
3. **The right to get data corrected:** you may question the accuracy of personal data held by the church, and ask for it to be corrected. If the data is incomplete you can ask for more details to be added. Rectification will only be possible where the data does not constitute historical records (e.g. correspondence, members' meeting minutes) which have to be maintained in their original form for the purposes of protecting the reputation of the church and its members and for reasons of safeguarding. It should be noted that if corrections are required to member's meeting minutes an opportunity is always given at the beginning of the following meeting when the minutes are read, beyond this the minutes become fixed historical records.
4. **The right to get data deleted:** you may request the 'erasure' or destruction of personal data, where there is no compelling reason for it to be retained. This is not an absolute right, and there may be circumstances where we have a legal obligation not to erase data, e.g. safeguarding. Also the right to 'be forgotten' cannot apply to any correspondence or church minutes that the church holds because of the church's responsibility to protect the reputation of the church, (its members and others in the congregation), and for reasons of safeguarding. The written request for erasure of data would also be retained as a record of the request to be 'forgotten' by the church. Personal data still needed for reasons connected with its original collection, (e.g. Gift Aid processing), cannot be erased.
5. **The right to limit how we use your data:** you can request this, for instance when there is a concern about its accuracy or how it is being used. This also includes the right to prevent us deleting your data. In that case we would retain but not use this personal data. This also includes the right to withdraw consent, where personal data was previously collected from you with your specific consent, (such as for inclusion of your contact details in a church directory - in that instance others on the list will be contacted and asked not to use that information, until a new directory can be issued).
6. **The right to data portability:** this right is unlikely ever to apply in our situation as it generally relates to the transfer of specific types of electronic data not handled by this church. Historical paper based records and documents are not included within this right.
7. **The right to object to the use of your data:** in certain circumstances individuals can object to their personal data being used, for instance if the church were to engage in direct marketing, (i.e. try to sell you something). Rest assured that we would never intentionally use your data in this way.

8. **Rights in relation to decisions being made about you without human involvement:** this would never arise because the church does not carry out any automated decision making.
9. **The right to access information from a public body:** Hope Church is not classed as a public body, so this right is not applicable.
10. **The right to raise a concern:** if you have specific concerns about how we are processing your data, you have the right to raise your concerns with us. If you then feel these concerns have not been addressed adequately, you also have the right to follow this up via the Information Commissioner's Office. For further advice see: https://ico.org.uk/your-data-matters/raising-concerns/

    Details of how to contact the church data manager in relation to any of these matters appear later in this document.
    General advice on your rights under GDPR can be seen at https://ico.org.uk/your-data-matters/

The right to get copies of your Data

(Subject Access Request)

To make a 'subject access request':

a. Contact the church data manager in person*, by email, post, or phone*; (*follow up verbal requests with letter or email to provide a clear record)
b. Make sure you include the following information:
1. state that you are making a 'subject access request';
2. your full name, address and contact telephone number;
3. any other relevant information used by the church to identify you such as gift aid reference number;
4. details of the specific information you require and any relevant dates;
c. If we need further details from you to locate the information you want, we will contact you, and will deal with your request when you have replied;
d. The church should reply within one calendar month starting from the date the request is received, and will provide the information you have requested, or inform you why we cannot do so. (Sometimes documents may also relate to other individuals, and in this case, their consent may need to be sought, or the document may be provided in a 'redacted' form);
e. There is normally no charge or fee for providing this information;
f. Further guidance can be found on the Information Commissioner's Office website https://ico.org.uk/your-data-matters/your-right-of-access/

Church Data Manager Details

Church Data Manager
Hope Church
Peacock Street
Gravesend
DA12 1EG

07583999974

admin@hopechurch.org.uk

Taking Care of your Data

There are several aspects to this:
1. Confidentiality and Security of Data
2. Lawful Use of Data
3. Integrity of Data

Confidentiality and Security:
1. Responsibility for keeping personal data safe lies with every individual that has legitimate access to and right to 'process' another individual's personal data. This includes church officers, members and other volunteers and employees. This duty is a legal requirement under UK Data Protection Law, and is a central aspect of this Data Protection Policy.
2. Personal data may be held in paper format, (including photographs), or electronic format, (including digital photos and videos).
3. At present there is no "church computer" or IT system storing "church data" as such. But paper based and digital information relating to the life of the church containing personal data may be held by different individuals within the church, stored in different ways, (e.g. in a filing cabinet, on a shelf, or on personal computers. Some personal data, for instance attendance registers for Junior Church, may also be stored on site at the chapel.
4. As a church our basic approach to confidentiality and security must be:
    a. to identify suitable measures that should be taken to ensure that personal data is kept safe;
    b. adopt these as formal church policy;
    c. to take actions designed to implement this policy;
    d. periodically to review whether the policy is working, and identify whether any further measures are required to ensure future adherence with the policy.
5. **Statement on Information Security**
    1. **Appointment of a Church Data Manager**
    - We will appoint a church data manager to oversee matters relating to Data Security. This is an unpaid position. They will be the first point of contact in any questions relating to how 'personal data' is being processed in the church. If they are unable to answer a specific question, they will seek appropriate advice from elsewhere.

    2. **Access to Personal Data:**
    - We will ensure that only those who have legitimate reasons to access data will be granted that access.

    3. **Paper-based documents at the Chapel:**
    - If documents containing personal data are distributed or used at the chapel, they should not be left lying around so that unauthorised people can view them;
    - Documents containing personal data stored at the chapel should be kept to a minimum;
    - Any such documents must be stored securely in a lockable filing cabinet or cupboard;
    - Keys will be issued only to those entitled to access these documents;
    - Confidentiality must be maintained whenever documents are in use;

- After use, any documents must be returned to their secure storage.

4. **Electronic personal data at the Chapel:**

- At the present time, no electronic computer systems storing personal data are in use at the chapel. If this situation should change this Policy Statement should be updated to reflect this change.

5. **Paper-based documents in private homes:**

- Members and Officers of the church should ensure that confidentiality is maintained when using or storing documents at home, especially when documents contain sensitive personal data. Choose an appropriate work area when viewing or using such documents, and put them away after use in a suitable filing system, so that others in your home not authorised to read personal data cannot accidentally view them.

6. **Electronic personal data on Personal Computers:**

- Access to any personal computer storing personal data should be password protected.
- If the computer is shared with others who should not have access to this personal data, ensure that there is a secure password protected area on your computer just for your use.
- Do not forward emails containing personal data to anyone who would not be authorised to view them or any associated attachments.
- Hope Church email addresses such as admin@hopechurch, treasurer@hopechurch are subject to the same guidelines. We will ensure that passwords for church email addresses are also held by a second church officer, so that information can be retrieved in the event of lost access.

7. **Destruction of Paper Documents and Deletion of Electronic Files:**

- The same consideration for the need for confidentiality should be exercised when disposing of documents that are no longer required. Paper records with personal or sensitive data should be shredded. If a shredder is not available, documents should be passed to the church data manager for shredding.
- When deleting electronic files, remember to delete any back up files and empty the recycle bin.
- If a personal computer is to be sold or otherwise disposed of, individuals should seek guidance from the church data manager, as personal data may still remain on the computer's hard drive.

8. **Third Party access to church data:**

- No personal data will be shared with any third party without their express consent, other than where required by law, e.g. safeguarding.
- We will ensure that where we do share such personal data by consent, (e.g. Stewardship payroll), that the third party is subject to its own valid Information Security Policy

9. **Training about Data Protection Principles**

- The leadership of the church undertakes to ensure that adequate instruction of all church members is carried out, so that everyone with access to personal church data remains familiar with the issues involved, and their responsibilities under the GDPR legislation.

10. Reviewing Data Protection Policy

- We will carry out regular reviews of this Policy on an annual basis, to ensure that it is still fit for purpose, to check what data is held and why, to highlight any issues, and to make recommendations about changes in our procedures, especially if any new data legislation is introduced.

11. Breaches of our Information Security Policy

- With the best will in the world, things can sometimes go wrong. If at any time anyone with responsibility for handling church data becomes aware that personal data or confidentiality has been compromised, by reason of accident, negligence or malicious intent on the part of others, (e.g. computer hacker), they should:
  i. report what has happened to the church data manager or another church leader
  ii. give full details of the breach
    - date and time of discovery
    - who discovered it
    - what data is involved
    - whose data is involved
- The church data manager should
  i. ensure that there is no ongoing breach
  ii. investigate what happened and determine the severity of the issue
  iii. consider taking further specialist advice if required and decide whether other authorities including the police or the Information Commissioner's Office need to be informed.
  iv. notify any individuals affected by the incident where appropriate
  v. review data security and decide if further measures are required
  vi. keep written notes of all actions taken

Lawful Use of Data

1. We will ensure that any personal data processed by the church is handled in accordance with one of the six Lawful Bases already described in this document.
2. Where **consent** is required from individuals before their data is used, we will issue a **Privacy Notice** when the information is collected, and ask for specific consent.

Integrity of Data

1. When we become aware that data is no longer up to date, we will review the ongoing need to retain it, whether we still have a lawful basis to process it, and will then amend it accordingly.
2. In addition we will regularly carry out checks to ensure that data held is still current, still lawful, and that we still have consent to process it where required.
3. We will action any requests to amend, delete, stop using, or provide copies of church data within one calendar month, (in line with GDPR rights). When we are unable to do so, or unable to do so within that timescale, we will provide written reasons why this is the case.
4. We will not retain data any longer than required, and only so long as this can be done lawfully. We will follow our **Data Retention Policy**

Data Retention Policy

1. Any paper document or digital file containing personal data is confidential in nature, and must be processed lawfully in accordance with GDPR principles. In particular this means that:
    a. There must be a legal basis for processing the data from the point at which it is collected;
    b. The data must be stored securely, in line with our **Statement on Information Security** guidance, and in an appropriate location with consideration given to the degree of sensitivity and confidentiality of the data, and also with regard to the frequency it will need to be accessed;
    c. There should be a good reason for ongoing retention of any data, justified by a clear ongoing legal basis, and regular checks that this is the case should be carried out as described below
2. Data and records should not be kept for longer than is necessary
    a. Some data can be legitimately retained on a permanent basis, such as historical minutes of church meetings.
    b. Some data will need to be retained for an indefinite period for the legitimate interests of protecting the reputation of the church, its members and volunteers, such as the names of children in membership of children's clubs.
    c. Other types of data will need to be retained for varying periods of time, depending on what it is and why it is being retained.
3. Deletion, destruction and disposal of redundant files and documents should be carried out in accordance with our **Information Security** guidance.
4. The following guidelines should be followed:

Types of Data	**Suggested Retention Period**
Employee personnel files, including training records and notes of disciplinary and grievance hearings.	• 6 years from the end of employment
Application forms/interview notes	• Maximum of one year from the date of the interviews for those not subsequently employed. • If employed, retain in personnel file.
Information relating to children NB. You may find it helpful to read the following article: https://christiansafeguardingservices.phasic-ltd.co.uk/record-retention	• Review accuracy once a year; • Record that child was a member of the group (name and DOB for identification purposes) – permanent; • Secure destruction of personal data other than name and fact of membership – maximum three years after child ceases to be a member –normally should be destroyed if child has ceased regular attendance and has not attended within three months, (can be done at annual review); • Activity consent forms-as above, but in cases of accident/serious incident, should be retained for up

	to three years. (NB It should be a condition of participation in activities that consent forms are completed prior to the event); • Safeguarding file raised- to be retained until child reaches age 25; • Record of an allegation made of abuse against a child where the allegation is not substantiated. Any record concerning the alleged abuser must not be retained and is to be destroyed immediately; • Record of an allegations made of abuse against a child where the allegation is substantiated. All records concerning the abuser must be retained for 10 years after death or normal retirement age if employed, or 10 years after the person ceases to volunteer. This applies even if the individual no longer has any connection to the church.
Church member information	• Review accuracy once a year; • Record that adult was a member – permanent; • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member;
Church group (where any such groups exist) -member information	• Review accuracy once a year; • Record that adult was a member of group – permanent; • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member.
Income Tax and NI returns, including correspondence with HMRC	• 6 years after the end of the financial year to which the records relate.
Statutory Maternity Pay records and calculations	• As Above; (Statutory Maternity Pay [General] Regs. 1986)
Statutory Sick Pay records and calculations	• As Above; (Statutory Sick Pay [General] Regs. 1982)
Wages and salary records	• 6 years from the tax year in which generated.
Accident books, and records and reports of accidents	• (for Adults) 3 years after the date of the last entry; • (for children) 3 years after the child attains 18 years (RIDDOR 1985).
Health records	• 6 months from date of leaving employment (Management of Health and Safety at Work Regs.)
Health records where reason for termination of employment is	• 3 years from date of leaving employment (Limitation period for personal injury) claims)

connected with health, including stress related illness	
Photography	• Photographs selected for use in church publicity, or as a historical record of church life will be retained permanently. • Other photographs may be retained for up to 3 years

Privacy Notices

1. Privacy Notice for Public Display

Under GDPR a Privacy Notice should be displayed publically, (such as on a notice board at church, and on the church website).

This has to state:

- The name of the organisation
- What data is being collected, why and how it is to be used
- The legal basis for collecting and using it
- Who the data will be shared with
- Individual rights under GDPR
- When the Data Protection Policy will be reviewed

So our Privacy Notice (display version) reads as follows:

Privacy Notice:

How Hope Church uses your information

Your privacy is important to us. We are committed to safeguarding the privacy of your information. It is important that you read this privacy notice together with any other privacy notices that we may provide from time to time when we collect personal data about you. This is so that you are fully aware of how and why we are using your data.

Data Controller

Hope Church is known as a 'Data Controller' in connection with its responsibility for your personal data.

Why are we collecting your data?

Hope Church exists for charitable and religious objectives, namely the advancement of the Christian faith. We collect personal data to help us provide appropriate pastoral care, to carry out a range of activities in pursuance of our objectives, in a safe environment and in compliance with the law. In legal terms this is called 'legitimate interests'. When it is required, we may also ask you for your consent to use your personal information. We do not share your information with others except as described in this notice.

The categories of information that we may collect, hold and share include:

- Personal information (such as name, telephone number, address and email address)
- Characteristics (such as gender, ethnicity, language, nationality, country of birth)
- Special categories of personal data (such as your religious beliefs)

Storing your data

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for. This may include for legal, accounting or reporting requirements.

We hold your data for varying lengths of time depending on the type of information in question, but in doing so we always comply with Data Protection legislation. Details of retention periods are available in our Data Retention Policy which you can request by contacting us at admin@hopechurch.org.uk

We will review the information we hold annually to ensure that it is still accurate.

Security of your data

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees or church officers who need to know. They will only process your personal data on our instructions. You can read more about this in our Statement on Information Security.

We have put in place procedures to deal with any suspected personal data breach and will notify you and the Information Commissioner's Office where we are legally required to do so.

Who do we share your information with?

We will not share your information with third parties without your consent unless the law requires us to do so.

Requesting access to your personal data

Under Data Protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the church data manager.
You also have the right to:

- object to the use of personal data that is likely to cause, or is causing, damage or distress
- prevent use of your data for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

For further information on how your information is used, how we maintain the security of your information and your rights to access information we hold on you please contact the church data manager.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/your-data-matters/raising-concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact the church by any of the following methods:

In person: Speak to the church data manager

By email admin@hopechurch.org.uk

By post Church Data Manager
Hope Church
Peacock Street
Gravesend
Kent DA12 1EG

By phone 07583999974

2. Adaptable Privacy Notice

When collecting information from someone a Privacy Notice also has to be given to the individual. The wording of this will depend on the information and why it is needed, but the basic elements remain consistent. As before:
This has to state:

- The name of the organisation
- What data is being collected, why and how it is to be used
- The legal basis for collecting and using it
- Who the data will be shared with
- Individual rights under GDPR
- When the data will be reviewed

Example: as part of Junior Church Registration Form

Privacy Notice: Hope Church

Here at Hope Church we care about your privacy. We are collecting this information to enable the church to run Junior Church safely and ensure we can contact you in case of an emergency.

UK Data Protection allows us to gather, use and store this information as it is in the church's legitimate interest. We will not share this data with anyone else unless obliged to by law.

The form you supplied will be kept in a locked cupboard in the chapel. Your child's name and date of birth will be transferred onto an attendance register which will also be kept in a locked cupboard. Only specified leaders will have access to this information.

The form will be retained for a period of 6 months after your child stops regularly attending Junior Church, or when they start remaining downstairs for our main service. We will then shred the form.
The attendance register will be retained indefinitely since it contains information about different children, and in line with our Safeguarding Policy.

Hope Church Privacy Notice is displayed on our notice board in the Chapel and on our website www.hopechurch.org.uk and this explains your legal rights. A copy of our Data Protection Policy is available on request. We review this Policy annually.

If you have any questions about this Privacy Notice please contact admin@hopechurch.org.uk

Appendix 1a Data Protection at a glance: Church Members/General Good Practice

General: "Each of you should look not only to your own interests, but also to the interests of others." (Philippians 2:4)

Verbal:
As a general principle we should all safeguard one another's privacy and personal data. For example, personal information should not be shared in church gatherings such as the prayer meeting without permission. If visitors or other non members are present in the meetings, there is no guarantee that sensitive personal data may be shared beyond the church membership.

Paper:
Treat all documents with your own or others personal details as confidential

- Don't leave any documents (e.g. minutes from church members meetings) lying around in the chapel or at home for others to pick up and read.
- This also applies to financial information about the church, as this is confidential anyway, and may also contain details from which personal information may be inferred, e.g. levels of giving, salary information etc.
- If you wish to destroy unwanted documents, make sure these get shredded and not just put in the bin

Digital:
In the same way treat all personal data received via the internet as confidential

- Password protect access to your computer
- Don't forward emails to anyone who is not authorised to read them.
- Be careful when sending on one email where it is part of a string of emails because the earlier emails written by others may contain personal data
- Be aware that attachments may contain personal data even if the email text does not
- For group email distribution it is recommended that you use bcc (blind carbon copy) for the address field, so that you will not be inadvertently disclosing other peoples email addresses
- When deleting digital data, remember to delete them from any backup and then empty the recycle bin also

Photography

- Photographs should only be taken by designated photographers appointed by the church leaders.

Data Loss or Theft

- If you become aware of any data breaches where personal data has been lost, stolen or compromised in any other way, (in either paper or digital format), please let one of the church leaders know straightaway, so a decision can be made about who else might need to be notified
- You may have to let your internet provider or the police know in the event of theft

Appendix 1b Data Protection at a glance: Church Officers

In addition to general advice given to Church Members in appendix 1a, church officers should also be aware of the special trust they enjoy.

Pastor/Elders

Treat sensitive personal data with special care:

- Store any written information securely, and password-protect access to any digital data.
- Review accuracy of data regularly in line with Data Protection Policy
- Destroy or delete any personal data after it is no longer required for the purposes of pastoral care in line with the Data Retention Policy
- When making official records (such as meeting minutes) ensure that only the minimum personal information necessary is recorded. For example, where possible, use names in an anonymous form, especially if referring to those who are not members of the church .

Treasurer

Treat sensitive personal data with special care:

- Gift Aid declarations, church bank statements, personal banking details and electronic records of giving to the church to be held securely at all times
- Ensure all correspondence with HMRC and Stewardship Ltd take place in confidence
- Review accuracy of data regularly in line with Data Protection Policy
- Destroy or delete any personal data after it is no longer required for HMRC or financial accounting purposes in line with the Data Retention Policy

Safeguarding Officer/Deputy/Administrator

Treat sensitive personal data with special care:

- Data gathered for DBS checks to be treated in confidence and all but the signed declaration form destroyed as soon as the check completed. Declaration form to retained securely.
- Any Safeguarding files raised to be retained securely for as long as prescribed under Safeguarding Policy and Data Retention Policy

Junior Church Leaders/ Youth Club Leaders/Toddler Group Leaders

Treat sensitive personal data with special care:

- Ensure that no child attends your group without the parent or legal guardian completing a consent form which should be given out on their first attendance
- Have the consent forms readily available during the session, but lock them away at the end
- Transfer the information from the consent form accurately onto the attendance register
- Lock the attendance register away securely at the end of the session
- Review accuracy of the personal data annually in line with Data Protection Policy
- Destroy documents with personal data securely in line with Data Retention Policy

HOPE CHURCH, GRAVESEND

This Data Protection and Privacy Policy was formally adopted at a Church Member's Meeting

Date of adoption: **Sunday 26 /01/2020**

Date due for review: **After 26/01/2021**