



## Hope Church – GDPR and Privacy Policy

*A Company Limited by Guarantee – Registered Charity No. 1132992*

*Working name: We Are Hope Church – Member of the Evangelical Alliance*

### 1. Introduction

Hope Church is committed to protecting the privacy, dignity, and security of all individuals who engage with our ministries, activities, and services. This Privacy Policy explains how we collect, use, store, and protect personal data in accordance with the **UK GDPR** and the **Data Protection Act 2018**.

We process personal data to support our mission, ensure safe ministry practice, comply with legal obligations, and maintain effective communication with our congregation, volunteers, staff, and community partners, including those who hire our church site for their activities.

### 2. Who We Are

Hope Church Registered Charity No. 1132992

Address: Hope Church, Vines Road, Diss, Norfolk IP22 4HG

Data Protection Officer (DPO): Office Manager Michelle Clarke

Email: [office@wearehopechurch.net](mailto:office@wearehopechurch.net)

Telephone: 01379 644223

### 3. What Personal Data We Collect

We may collect and process the following categories of personal data:

- Contact details (name, address, email, phone number)
- Pastoral information shared voluntarily
- Safeguarding records
- Volunteer and staff information
- Attendance records
- Financial giving information
- Photographs and video recordings (with consent)
- Website and digital communication data
- Children who attend any Hope Church activities – names, ages and any allergies, emergency contact details for their responsible adults in case of emergency.

- Medication and instructions for those attending residential church events e.g. the youth who attend New Day in July annually.

We may, in further dealings with you, extend this information to include any information we think is required:

- You are under no statutory or contractual requirement or obligation to provide us with your personal information; however, we require at least the information above in order for us to deal with you in an efficient and effective manner.
- The legal basis for processing your data is based on your specific consent, performance of a contract if you are a hirer, compliance with a legal obligation, your vital interest, our legitimate interest that we will have stated to you at the point the information was initially provided. Therefore, we will not store, process or transfer your data outside the parties detailed above unless we have an appropriate lawful reason to do so.
- We may contact you following your enquiry to reply to any questions, suggestions, issues or complaints you have contacted us about
- If needed for emergency contact

#### **4. How We Use Personal Data**

We use personal data for:

- Pastoral care and ministry support
- Safeguarding children and adults
- Managing volunteers and staff
- Communication about church activities
- Legal compliance (e.g., safeguarding, charity law)
- Financial administration
- Event management
- Maintaining safe and effective operations

For those hiring part and/or all of our premises:

- We will make available our products and services to you
- Process your request
- Take payment from you or give you a refund

- We may provide you with details of products that match a product, which you may have purchased or enquired about previously
- We may contact you about products and services from us;
- Help answer your questions and solve any issues you have.

## 5. Lawful Bases for Processing

We rely on the following lawful bases:

- **Consent**
- **Legitimate interests**
- **Legal obligation**
- **Contract**
- **Vital interests** (e.g., safeguarding emergencies)

## 6. Sharing Personal Data

We only share personal data when necessary and lawful, including:

- With statutory agencies for safeguarding
- With service providers (e.g., IT, payroll)
- With emergency services
- With denominational bodies when required

We never sell personal data.

## 7. Your rights over your information

a) You have the right to access the personal information that we hold about you in many circumstances, by making a request. This is sometimes termed 'Subject Access Request'. If we agree that we are obliged to provide personal information to you (or someone else on your behalf), we will provide it to you or them free of charge and aim to do so within 30 days from when your identity has been confirmed.

We would ask for proof of identity and sufficient information about your interactions with us that we can locate your personal information.

If you would like to exercise this right, please contact us as set out below.

### b) Right to Correction Your Personal Information

If any of the personal information we hold about you is inaccurate or out of date, you may ask us to correct it. If you would like to exercise this right, please contact us as set out below.

### c) Right to Stop or Limit Our Processing of Your Data

You have the right to object to us processing your personal information if we are not entitled to use it anymore, to have your information deleted if we are keeping it too long or have its processing restricted in certain circumstances. If you would like to exercise this right, please contact us as set out below.

d) For more information about your privacy rights

The Information Commissioner's Office (ICO) regulates data protection and privacy matters in the UK. They make a lot of information accessible to consumers on their website, and they ensure that the registered details of all data controllers such as ourselves are available publicly. You can access them here <https://ico.org.uk/for-the-public>.

You can make a complaint to the ICO at any time about the way we use your information. However, we hope that you would consider raising any issue or complaint you have with us first. Your satisfaction is extremely important to us, and we will always do our very best to solve any problems you may have.

### **8. How the church may keep you updated on our services or our hiring guidelines:**

We will send you information about our church and what we offer by email or by using Churchsuite. This will only happen if you have previously consented to receive these communications. When you register with us an individual and/or hirer, you will be asked if and how you would like to communicate. You can change these choices over the phone or in writing/email at any time.

Please contact [office@wearehopechurch.net](mailto:office@wearehopechurch.net) for any concerns or queries around this matter.

### **9. Data Security**

We use appropriate technical and organisational measures to protect personal data, including:

- Secure digital storage – Churchsuite, Microsoft 365 and iKnowsafeguarding
- Access controls
- Encryption
- Staff and volunteer training
- Regular audits

### **10. Data Retention**

We retain data only as long as necessary for legal, safeguarding, or operational purposes. Safeguarding records follow statutory retention periods. Please see Safeguarding Records Management Policy.

## 11. Helpful documents

In Appendix 1 there is Data Processing Impact Assessment. Each ministry lead and lead of any Hope Church project should fill this in and return it to the church office and DPO will check this and then file confidentially.

In Appendix 2 there is easy to use document for managing any data breaches.

In Appendix 3 is a Data Breach Log for use of the DPO. Any data breaches must be reported to the DPO immediately.

## 12. Contact

For any data protection queries, contact:

### Data Protection Officer

Email: [office@wearehopechurch.net](mailto:office@wearehopechurch.net)

Phone: 01379 644223

| Document History and Version Control Table |                                                      |                    |              |
|--------------------------------------------|------------------------------------------------------|--------------------|--------------|
| Version                                    | Action                                               | Approval authority | Action date  |
| 1.0                                        | Document produced in accordance with GDPR guidelines | Trustees meeting   | May 2018     |
| 1.01                                       | Annual review                                        | Office staff       | June 2019    |
| 1.02                                       | Annual review                                        | KB                 | June 2020    |
| 1.03                                       | Annual review                                        | KB                 | June 2021    |
| 1.04                                       | Annual review                                        | KB                 | June 2022    |
| 2.01                                       | In response to Safeguarding audit September 2026     | TK                 | October 2026 |

## Appendix 1 – Data Protection Impact Assessment (DPIA) Template

A DPIA must be completed for any church activity, ministry, event, or process involving personal data.

### **1. Project / Activity Details**

- Ministry / Event Name:
- Lead Person:
- Date:
- Description of Activity:

### **2. Purpose and Lawful Basis**

- Why is personal data needed?
- Lawful basis:
- Special category data involved?

### **3. Data Collected**

- Types of data:
- Source of data:
- Volume and sensitivity:

### **4. Risks Identified**

- Potential harm to individuals:
- Likelihood and severity:
- Safeguarding implications:

### **5. Mitigation Measures**

- Security controls:
- Access restrictions:
- Training required:
- Data minimisation steps:

### **6. Approval**

- Completed by:
- Reviewed by DPO:
- Date approved:

## **Appendix 2 – Data Breach Response Procedure**

A data breach includes any incident where personal data is lost, accessed, disclosed, altered, or destroyed without authorisation.

### **1. Identify**

- Recognise or suspect a breach
- Preserve evidence
- Notify the DPL immediately

### **2. Contain**

- Stop further data loss
- Secure systems
- Change passwords
- Restrict access

### **3. Assess**

- What data is affected?
- Who is impacted?
- Risk of harm?
- Safeguarding concerns?

### **4. Notify**

- ICO within 72 hours if required
- Affected individuals if high risk
- Trustees if serious
- Document all decisions

### **5. Review**

- Lessons learned
- Update procedures
- Additional training
- Prevent recurrence

## **Appendix 3 – Data Breach Log Template**

This log must be completed for **every** breach or suspected breach.

**Incident Details**

- Date & Time:
- Reported By:
- Description of Incident:

**Data Involved**

- Type of data:
- Number of individuals affected:
- Special category data?

**Actions Taken**

- Containment steps:
- Notifications made:
- ICO reference number (if applicable):

**Outcome**

- Impact assessment:
- Follow-up actions:
- Final resolution date: