



Data Protection Policy

In May 2018 the regulations concerning data protection GDPR (General Data Protection Regulation) changed. The Community of Hopeweavers has produced a Data Privacy policy to conform with the new regulations.

There is a named Community Member (Paul Lambert) who takes responsibility for data protection compliance.

The Community of Hopeweavers:

- recognises and understands the importance of protecting personal information and the privacy of the data provided to them by Members, Enquirers, Friends and those booking for Community events;
- complies with its legal obligations by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

Data Controller: Trustees

Type of personal data	Who the data relates	How data is collected, stored & destroyed	Purpose of the data	Who has access to the data?
Name, postal address, email address, telephone number Church contact References Safeguarding training records	Trustees	Information is provided by the Trustee. References sought by the Guardians References are stored in the Office 365 environment Safer recruitment data is deleted 6 years after the trustee finished their last term of office.	Safer recruitment Returns to the Charity Commission. Ensure that Trustees have undertaken safeguarding training and have regular updates	Guardians Safeguarding Lead & Officer
Name, postal address, email address, telephone number	Members of the Community	Data is provided on the annual membership form (completed via survey monkey). It is stored in the Office 365 environment. When a member leaves the information is permanently deleted* from the spreadsheet after 3 years.	Provision of regular news and information about the community. Details of forthcoming events. Information given to group leaders to arrange meetings. Annual renewal request. Welfare checks.	Guardians and Trustees (must ensure that the access is removed when Trustees or Guardians step down) Group Leaders will hold their own contact details for members of their groups.



Data Protection Policy

Names, postal address, email address, telephone number	Enquirers to the Community	Data is provided by the Enquirer to the Community at their initial expression of interest. Information is stored in our Office 365 environment and emails of the Guide and Enquirer Administrator. If the enquirer decides not to continue their relationship with the community the information is deleted.	Provision of regular news and information about the community. Details of forthcoming events. Information given to their Guide for arranging meetings. Welfare checks.	Guardians and Enquirer Administrator
Name Email address	Friends of the Community	Data is stored in Mailchimp with GDPR protection. The unsubscribe option is always available.	Provision of regular news and information about the community. Details of forthcoming events.	Member with responsibility for data protection, Hopeweavers Administrator and Newsletter Administrator
Name and contact details Record of giving	Regular financial supporters	Data is stored in the Office 365 environment.	Financial planning purposes.	Treasurer
Name Email address Dietary requirements Disability information	Attendees at events	Stored in Eventbrite and by Event Leaders	Communication regarding the event / booking, particularly in the event it is necessary to cancel.	Host of the event
Information pertaining to any concerns raised about members and any subsequent investigation and action taken.	Members of the community	Data is stored within the 365 environment The length of time the information is kept will be related to the seriousness of the concerns and be determined by those leading the investigation.	Ensuring a safe community and ensuring a record of the actions taken to do so by those in a leadership position.	Accessibility to the information will be limited to those with a need to access it as determined by those leading the investigation.



Data Protection Policy

*information which is just 'deleted' can be accessed via reviewing previous versions of the document

Sharing your personal data

Your personal data will be treated as strictly confidential and will only be shared with other members of the team and Community to carry the above purposes. It will never be sold or given to other 3rd party organisations for marketing purpose.

How long do we keep your personal data?

Specifically, The Community of Hopeweavers retains data on booking forms for participants of Quiet Days and Soul Days for a period of 3 years. The forms are then destroyed. Financial data is held within the online banking system for 7 years following the person no longer being a donor.

Your rights and your personal data

Unless subject to an exemption under the GDPR, an individual has the following rights with respect to his/her personal data: -

- The right to request a copy of your personal data which the Community of Hopeweavers holds about you within a period of one month;
- The right to request that the Community of Hopeweavers corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the Community of Hopeweavers to retain such data;
- The right to withdraw your consent to the processing at any time
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data including processing for the purposes of scientific/historical research and statistics
- The right to lodge a complaint with the Information Commissioners Office.

Further processing

If the Community of Hopeweavers wishes to use your personal data for a new purpose, not covered by this Data Protection Notice, then you will be provided with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, The Community of Hopeweavers will seek your prior consent to the new processing.

Contact Details

To exercise all relevant rights, queries or complaints please in the first instance contact the Community of Hopeweavers using contactus@hopeweavers.org.uk

Subject Access Requests

- In most cases the Community of Hopeweavers will not be able to charge for complying with a request.
- The Community of Hopeweavers will have a month to comply.
- The Community of Hopeweavers can refuse or charge for requests that are manifestly unfounded or excessive.
- If the Community of Hopeweavers refuses a request, the individual must be told why and that he/she has the right to complain to the supervisory authority and to a judicial remedy. This must be done without delay and at the latest, within one month.

Subject access requests may be made in writing directly to contactus@hopeweavers.org.uk. All leaders will be asked what information is being held and its location. If the Community of Hopeweavers refuses a request, the



Data Protection Policy

individual must be told why and that he/she has the right to complain to the supervisory authority and to a judicial remedy. This must be done without delay and at the latest, within one month.

Data Breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO (Information Commissioners Office), and in some cases, to individuals. The ICO must be informed of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

All Members are requested to monitor their personal online accounts for references to the Community and its ministry. Possible breaches of confidentiality should be reported as soon as possible to the Community's data protection Member, for further investigation.

The advice of the ICO will be sought on where, and to what extent, the Community needs to inform a user of a data breach.

The Community has 72 hours to inform a person of a data breach.

Date of first risk assessment:	7/4/2018
Date of Last Update:	19/09/2024
Name of leader with responsibility:	Paul Lambert
Date to be reviewed:	May 2026