Place for Hope Privacy Notice (general)

Data controller: Place for Hope

The person with responsibility for data protection compliance is the Director.

The organisation collects and processes a variety of personal data relating to employees, volunteers, job applicants, people who provide it with services and people who use the services that it provides. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations. Details are contained in its Data Protection Policy and in its Privacy Notices.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether those interests are overridden by the rights and freedoms of data subjects and has concluded that they are not.

Employees

Please refer to Place for Hope's separate Employee Privacy Notice.

Practitioners

Please refer to Place for Hope's separate Practitioner Privacy Notice.

People who volunteer

In addition to volunteer Practitioners, information about which is detailed in the Practitioner Privacy Notice, the organisation collects and processes a variety of personal data relating to other volunteers, including Trustees. This may include name; contact details including email and telephone number; date of birth; national insurance number; nationality; employment; directorships and business interests; other trusteeships; and membership of organisations. It may also include special category data on religious affiliation to ensure a mix of faith community representation on the Board of Trustees under the condition of legitimate activity of a not-for-profit body with aims relating to religion.

The organisation collects this information from volunteers directly in a variety of ways, e.g. declaration of interest form, email. Data is stored in a range of different IT systems (including the organisation's email system) and shared internally by staff as necessary for performance of their roles. The organisation only shares volunteer data with third parties with consent and if required for the volunteer to fulfil agreed roles within the organisation, e.g. a Trustee who is a bank account signatory.

In some cases, the organisation needs to process volunteer data to ensure that it is complying with its legal obligations, e.g., to maintain an up-to-date Trustee Register. The organisation has a legitimate interest in processing other data, such as contact details, to maintain the volunteering relationship.

The organisation will hold personal data for the duration of the data subject's volunteering period. Some personal records, such as those provided for the Trustee Register may be retained 7 years after the period of service.

Some volunteers may have obligations to provide the organisation with data, e.g. Trustees. Certain information, such as contact details, are needed to work with all volunteers. Failing to provide such data may make it difficult or impossible to use someone's services as a volunteer.

People who apply for jobs

The organisation collects a range of information about job applicants. This may include name; contact details including email and telephone number; details of qualifications, skills, experience and employment history; whether or not the applicant has a disability for which the organisation needs to make reasonable adjustments during the recruitment process; information about entitlement to work in the UK; and information about religion, either provided voluntarily as part of an application or because required in accordance with the Equality Act 2010 Sch. 9, Para 3. The organisation collects this information in a variety of ways. For example, data might be contained in application forms, obtained from a passport or other identity document, or collected through interviews or other forms of assessment. Data will be stored in IT systems (including email). Copies of application forms may be stored in hard copy to aid recruitment processes.

The organisation has a legitimate interest in processing personal data during the recruitment process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The organisation may also need to process data from job applicants to respond to, and defend against, legal claims. The organisation processes health information, which is a special category of data, if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to recruitment for employment. The organisation processes information about religion, which is a special category of data, for any role for which it is an occupational requirement to be a member of a faith community in accordance with the Equality Act 2010 Sch. 9, Para 3.

The organisation will not use an applicant's data for any purpose other than the recruitment exercise for which they have applied. Personal data will be shared internally for the purposes of the recruitment exercise. This includes the Director, interviewers involved in the recruitment process, and other staff if access to the data is necessary for the performance of their roles. Recruitment processes are not based on automated decision-making.

The organisation will hold the data of unsuccessful applicants on file for six months after the end of the relevant recruitment process. At the end of that period the data will be deleted or destroyed. For a successful applicant, personal data gathered during the recruitment process will be transferred to their personnel file and will fall under the Employee Privacy Notice.

Applicants are under no statutory obligation to provide personal data to the organisation during the recruitment process. However, if they do not provide the data, the organisation may not be able to process their application properly or at all. Except in the case of jobs which require the post holder to be a member of a faith

community in accordance with the Equality Act 2010 Sch. 9, Para 3, there is no expectation that applicants should provide information about their religion or belief on application forms and there are no consequences of not doing so.

People who use training and support services

Place for Hope offers various training and support services to the public. Organisations or individuals can contact us about this in a variety of ways, including via phone, email and in person. The organisation has a legitimate interest in processing personal data of those who contact it about services and others in their organisations, such as members of the local faith community needing training or support, to provide these services. Data processed includes contact details, role and in some cases faith affiliation provided by the client and relevant parties during the initial enquiry and subsequently. Data on faith affiliation normally relates to a client organisation rather than to individuals. Where the organisation processes special category personal data on the religious affiliation of individuals, this is either as part of the legitimate activity of a not-for-profit body with aims relating to religion, or by consent.

The organisation only uses personal data to provide the service requested, to deliver our purposes as a registered charity, or for other closely related purposes, e.g. to contact people who have received training to let them know about other similar training courses which might be of interest to them.

The organisation will review every 5 years whether it is still important for delivering our purposes to continue to hold personal data. Data subjects can ask for its erasure at any time. Both electronic and any manual copies of data will be destroyed at the time of erasure.

The organisation may have to share personal data with third parties where we are legally required to disclose or report specific matters should they arise in the course of our work, e.g. for safeguarding. The organisation sometimes uses third-party providers to manage payments or bookings, e.g. Stripe or Eventbrite.

The organisation provides anonymised statistical information to our funders. The organisation uses attributed quotes from feedback in our marketing and promotional material only with explicit consent.

People who wish to use training and support services are under no obligation to provide personal data to the organisation. However, if they do not provide this, the organisation may not be able to provide the requested service.

People contracted to supply specific services

Place for Hope processes personal information, including contact and other details, provided by those who it contracts to provide various kinds of consultancy support, for example supervision, HR, accountancy, and payroll services. The organisation uses this personal data to deliver its purposes as a registered charity, and for other closely related purposes. The organisation has a legitimate interest in collecting this data to make use of the service provided under the contract or other agreement. This personal information will be retained by the organisation until the end of the consultancy arrangement, and for up to 5 years afterwards in case it wishes to use

the consultancy service again. Data subjects can ask for its erasure at any time after the end of the consultancy period.

People who sign up to the Peacemakers Network

Place for Hope processes the personal data of those who sign up to join the Peacemakers Network mailing list. The organisation processes this data by consent for the purpose of keeping Peacemakers Network members informed about its news, work, and events through an e-newsletter. Personal data collected includes contact details and in some cases role and faith affiliation if provided voluntarily on the online sign-up form or by signing up at events. This helps to tailor the e-newsletter and deliver the organisation's purposes as a registered charity. This personal data is retained until the data subject opts out of receiving the e-newsletter, after which it will be destroyed unless the organisation seeks and receives consent to retain it for another purpose. The organisation uses a third-party provider, Mailchimp, to deliver e-newsletters. The organisation reviews statistics around email opening and clicks using industry standard technologies provided by Mailchimp to help monitor use of and to make improvements to the e-newsletter.

People who contact us via social media

Place for Hope uses a third-party provider, Hootsuite, to manage its social media interactions. Private or direct messages from those who contact the organisation via social media are stored by Hootsuite for three months. Messages are not shared with any other organisations.

Visitors to our website

Place for Hope uses a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns on www.placeforhope.org.uk to find out things such as the number of visitors to the various parts of the site. This data is anonymised. The organisation does not make, and does not allow Google to make, any attempt to find out the identities of those visiting its website. If the organisation wishes to collect personally identifiable information through the website, it will be transparent about this and seek consent, making it clear when personal data is sought and explaining how the data will be used. The website uses cookies.

Review

This privacy notice will be reviewed annually.

Data Protection Policy

Introduction

Purpose

The organisation is committed to being transparent about how it collects and uses the personal data of its workforce and clients, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, former employees, and clients, including parties to interventions and trainees.

The organisation has appointed the Director as the person with responsibility for data protection compliance within the organisation. They can be contacted at info@placeforhope.org.uk. Questions about this policy, or requests for further information, should be directed to the Business Development Manager or Director at this email address.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The organisation processes HR-related personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices, and when collecting data where consent is required. It will not process personal data of individuals for other reasons. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

The organisation will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Where the organisation processes special categories of personal data this will generally be either as part of the legitimate activity of a not-for-profit body with aims relating to religion, or by consent.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the following policy on special categories of data and criminal records data:

- The organisation will process only those types of special category data that are necessary for the purposes of its rights and obligations in employment law, for example in regard to monitoring and managing sickness absence.
- The organisation will use this data only in accordance with the purpose for which it is collected.
- The organisation will process criminal record data only where this is permitted by law and necessary for the organisation, for example for vetting individuals as part of the recruitment process.

Personal data gathered during employment is held in the individual's personnel file in hard copy or electronic format, or both. The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If you make a subject access request, we will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom your data is or may be disclosed;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the organisation has failed to comply with your data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless you agree otherwise.

To make a subject access request, send the request to info@placeforhope.org.uk. In some cases, we may need to ask for proof of identification before the request can be processed.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. We will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

Other rights

As a data subject you have a number of other rights in relation to your personal data. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact info@placeforhope.org.uk.

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner. Be aware that the employer does not have to erase data that they need under UK law or where it is necessary to establish or defend legal claims.

Data security

The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees or volunteers in the proper performance of their duties. Electronic devices used to store data are password protected. Encrypted systems such as Dropbox and Salesforce are used for the storage of data.

Where the organisation engages third parties to process personal data on its behalf, it ensures that such parties also adhere to a high level of security and confidentiality with regard to this data.

Data breaches

If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

The organisation will not transfer personal data to countries outside the UK or EEA.

Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual changes contact details or an employee or volunteer changes their bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, or volunteer period. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;

- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on computer access, including password protection, and secure file storage and destruction);
- adopt appropriate security measures (such as encryption or password protection) to secure personal data, or devices containing that data or used to access personal data, when working from home and elsewhere; and
- to report data breaches of which they become aware to the Director immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The organisation will provide appropriate training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Retention Periods

The periods for which the organisation holds personal data are contained in its privacy notices. After these periods, both manual and electronic records shall be destroyed securely.

Policy review

This policy will be reviewed annually.

Revised May 2021