

Place for Hope Practitioner Privacy Notice

Place for Hope (Charity Number: SC045224) (“our” or “we” or “the organisation”) act as a data controller in respect of your personal information and this means that we are responsible for deciding how we hold and use personal information about you. We collect and process personal data relating to our Practitioners to manage the volunteer relationship. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

This Privacy Notice applies to current and former Practitioners (also referred to as “you” or “your”). Please note that this Privacy Notice does not form part of the Mutual Agreement or any other volunteer agreement with you.

The person with responsibility for data protection compliance is Helen Boothroyd: helen.boothroyd@placeforhope.org.uk. For any data breaches involving Practitioners or complaints about how your personal data has been handled, please contact the Director Georgia Boon: georgia.boon@placeforhope.org.uk; 07557 869924.

What is ‘personal information’?

Your 'personal information' means any information about you from which you can be identified - either by reference to an identifier (for example your name, location data or online identifier (e.g. IP address) or from factors specific to your physical, cultural or social identity (e.g. your social background, outside interests etc).

It does not include information where the identity has been removed (such as anonymous information).

What personal information do we collect and process?

We collect and process a range of information about you. This includes, but is not limited to:

- your name, address and contact details, including email address and telephone number; gender, next of kin and emergency contact information;
- photographs / film footage;
- details of your relevant training, qualifications, skills, experience, employment history and current employment; and start and end dates with the organisation;
- details of your bank account;
- details of when you undertake work for the organisation;
- notes and other documentation from casework you undertake for the organisation, including emails, stored on our database;
- health and safety information (this can form photographs, videos, investigation notes, health reports, witness statements); and
- information in relation to CPD, support and supervision.

‘Special Category’ Information

We also collect and process ‘special category’ information about you, which is information that is more sensitive (such as information about racial/ ethnic origin, sexual orientation, political opinions, religious/ philosophical beliefs, trade union membership, biometric or

genetic data and health data) and given a higher level of data protection laws. This may include (but is not limited to):

- information about medical or health conditions, including whether or not you have a disability for which we need to make reasonable adjustments;
- information about your religion if you provide this voluntarily; and
- information about your racial/ethnic origin if you provide this voluntarily.

How do we collect personal information?

We collect this information in a variety of ways. For example, data is collected through application forms, from correspondence with you, or through interviews, meetings, or other assessments.

In some cases, we collect personal data about you from third parties, for example from Supervisors.

What is the legal basis?

In most cases, we will process Practitioner's personal information where it is necessary:

- to perform the Mutual Agreement we have entered into with you for the purposes of the volunteering arrangement – **Basis 1**
- to ensure that we are complying with our legal obligations (for example to comply with health and safety laws) – **Basis 2**
- for our legitimate interests in processing personal information before, during and after the end of the your relationship with the Organisation – **Basis 3**;
- when we have obtained your consent (for example, if we are making travel or accommodation arrangements on your behalf we will pass this information to the travel or accommodation providers) – **Basis 4**.

Where we rely on legitimate interests as a reason for processing personal information, we have considered whether or not those interests are overridden by the rights and freedoms of Practitioners and we have concluded that they are not. Our legitimate interest is the purpose for which we process the data (e.g. for data we process during the recruitment process, the legitimate reason for processing that data is recruitment).

We may also process your personal information in the following circumstances, but this is likely to be rare:

- with specific consent;
- where it is necessary to protect your interests (or someone else's interests);
- where it is needed in the public interest.

If we are processing special category data we may also rely on the following conditions in addition to the legal bases above:

- where you have given your consent to the use of your data;
- where we are required to process your data in the public interest for the purposes of regulatory requirements relating to unlawful acts and dishonesty;
- where we are required to process your data in the public interest for the purposes of equal opportunities or treatment.

What is the purpose for processing your personal information?

Processing your personal information allows us to do a number of different purposes, including (but not limited to):

- run volunteer recruitment processes;
- maintain accurate and up-to-date records and contact details (including details of who to contact in the event of an emergency);
- allocate cases to ensure you are deployed appropriately;
- operate and keep a record of CPD, support and supervision;
- ensure effective general HR and business administration;
- provide references on request for current or former Practitioners;
- comply with our legal obligations, such as health and safety laws;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

We will only use your personal information for the purposes for which we collected it - unless we reasonably consider that we need to use it for another purpose that is compatible with the original purpose.

If we need to use your personal information for an unrelated purpose, we will notify you and explain the basis upon which that is necessary.

What is the purpose for processing 'special category' personal information?

Some special categories of personal information, such as information about your health or medical conditions and about your religious beliefs, are processed as part of the legitimate activities of the organisation as a not-for-profit organisation deploying you to work with faith communities. You are free to decide whether to provide such data when requested, on application forms or subsequently. We may process information about your racial/ethnic origin in order to monitor the diversity of our practitioner team, but only with your explicit consent.

Consent

We will only seek and rely on your consent where you are fully informed and your consent can be freely given.

There may be limited circumstances where we will approach you to obtain your explicit consent to allow us to process certain particularly sensitive data, or other personal information.

If so, we will provide you with full details of the information that we require and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that you do not have to provide your consent and it will not impact on your Mutual Agreement with us if you do not consent.

You have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for that purpose.

If you wish to withdraw your consent, please contact Natalie Barrett:
natalie.barrett@placeforhope.org.uk.

Who do we share your personal information with?

The organisation will share your personal information internally, including with those who manage your work, and with other staff if access to your personal information is necessary for performance of their roles.

Third Parties

We contract with third party service providers and suppliers to deliver certain services, such as supervision. Our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We are also legally required to transfer certain data to governmental and regulatory bodies.

We may share your personal information data with third parties in order to get pre-selection references.

We may also share your personal information with third parties that process data on our behalf, predominantly in connection with expenses payments.

The following third parties may have access to your personal information for the purposes noted below:

- Microsoft hosts our emails on Outlook in Office 365 and any documents stored to Office 365 applications, processing personal data in the UK;
- Dropbox hosts our file storage, processing personal data in the US;
- Mailchimp, which we use for e-newsletters, processing personal data in the US;
- Salesforce hosts our cloud-based database, processing personal data in the UK and US;
- Hootsuite manages our social media interactions, processing personal data in the UK and Canada;
- third-party providers to manage payments, bookings or registrations, e.g. Stripe, Eventbrite, and Google suite, processing personal data in the UK, EU, and US;
- third-party providers to manage our website functions, e.g. Expression Engine and Google Analytics processing personal data in the UK, EU, and US;
- Intego, which is our anti-virus provider, processing personal data in the UK and US;
- Vodafone which is our mobile telephone provider;
- Easybooks accounting system, processing personal data in the UK and US;
- our independent examiner and accountant who is currently Paul Clelland Accountancy, processing personal data in the UK;
- our insurance providers who are currently Keegan and Pennykid, processing personal data in the UK;

- our current account banking providers who are currently CAF Bank, processing personal data in the UK;
- our funders or other grant providers where required e.g. personal information for funding applications or required for reporting on outcomes and outputs;
- any other person who is authorised to act on your behalf (for example, the NHS and/or family members);
- any relevant dispute resolution body or the courts;
- persons or organisations in connection with any merger, disposal, reorganisation, or similar change in our charity;
- regulators, government departments, law enforcement authorities, tax authorities, professional advisers, financial institutions, and insurance companies;
- third parties providing a reference about you, where you have agreed that we can request this or have asked us to request it;
- if you require a reference, we will provide your information to the other body to whom you have asked us to supply it.

Our service providers change from time to time and we will inform you if this is the case. We will not sell, trade or lease your personal information to others.

Legal Basis

In most cases, we will share your personal information with third parties where:

- required by law
- it is necessary to administer the working relationship with you, or
- we have another legitimate interest in doing so, for example as part of a relationship with a funding partner.

In these circumstances, we require third parties to ensure the security of your personal information and to treat it in accordance with the law.

How do we keep your personal information secure?

Data is stored in a range of different IT systems (including the organisation's email). We use encrypted systems for online processing and storage and anti-virus protection on all staff laptops. All laptops and mobile phones used by our staff are password protected with auto-lock facilities enabled. Email security is a priority, and staff and practitioners are asked to avoid sharing personal information by email.

Our password policy requires:

- The use of complex passwords which would be hard to guess;
- Secure password storage;
- Password sharing between staff as an exception, only where operationally necessary and never regarding the storage of financial or other sensitive information;
- Additional security for financial and other sensitive information, including only password hints being held in secure storage and multi-factor authentication.

Personal information is only accessible to staff members who require it to perform their role. Personal information is only shared with volunteers, e.g. practitioners, trustees or volunteers assisting with financial systems, only where a specific piece of information is

required for the task they are being asked to perform. Volunteers do not have access to our database.

Personal information is not generally held in hard copy. Any hard copy personal information that is required to be held is:

- stored by only one person if possible;
- stored in a locked container;
- shredded at the end of the retention period.

For how long does the organisation keep personal information?

The following timescale outlines the retention and disposal of Practitioner records:

- a Recruitment Records – held for full duration of the volunteering period and for a period of up to 7 years after the Practitioner has ceased to volunteer with us;
- b Personal files – retained 7 years after the Practitioner has ceased to volunteer with us;
- c Finance Records – retained 7 years;
- d Certain records held for a number of years after the Practitioner has ceased to volunteer with us. For example:
 - Health and safety records – up to 10 years or more depending on the type of record
 - Any records which may be required to prepare for, or defend, a legal claim.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

What if you do not provide personal data?

You have some obligations under the Mutual Agreement to provide us with personal data. Certain information, such as contact details, have to be provided to enable us to enter into the Mutual Agreement with you and to carry out our work. Failing to provide the data may make it difficult to use your services as a Practitioner. If you fail to provide certain information when requested, we may not be able to perform our obligations to you under the Mutual Agreement (such as paying your expenses).

Your rights in relation to your personal information

You have rights in relation to the personal information that we hold about you, including the right:

- to request access to any personal information we hold about you - or in some cases, to obtain a portable copy of it or to have it transferred to a third party;
- to ask to have inaccurate data amended;

- to erase your personal information, or to restrict or challenge the processing of your personal information in limited circumstances;
- to object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms;
- to request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
 - (a) if you want us to establish the data's accuracy;
 - (b) where our use of the data is unlawful but you do not want us to erase it;
 - (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it;
- to withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent;
- to lodge a complaint with the Information Commissioner's Office (the UK supervisory authority for data protection issues)

If you want to make one of these requests, please put your request in writing to Natalie Barrett: natalie.barrett@placeforhope.org.uk.

Please note, we may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We may not always be able to comply with your request to exercise your rights for specific legal reasons which will be notified to you, if applicable, at the time of your request.

If a data subject access request (DSAR) is manifestly unfounded or excessive, we are 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 DSAR is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If we consider this to be the case, we will notify you of this and of whether or not we will respond to the request.

Where do we store your personal information?

The data that we collect from you will usually be stored inside the UK or the European Economic Area (EEA).

However, if you live or work outside of the UK or the EEA, we may need to transfer your personal data outside of the UK or the EEA to correspond with you. If we organise

international travel on your behalf we may be required to provide information to providers and government bodies based outwith the EEA.

We also may transfer data outside the UK or the EEA where our service providers host, process, or store data outside the UK or the EEA. Where we do this, we will ensure that the transfer is to a country covered by a decision of the UK and/or European Commission or is otherwise made in circumstances where appropriate safeguards are in place to protect your data in accordance with the UK data protection legislation (e.g. standard contractual clauses, EU-US Privacy Shield compliant, etc.).

Review

This privacy notice will be reviewed annually, but we may update, or otherwise amend, this Privacy Notice at any time.

This document was last updated on 10 November 2021. It was considered and recommended for approval by the Policy and Practice Forum on 15 November 2021 and approved by the Board of Trustees on 7 December 2021.

Contact

If you have any questions regarding this Privacy Notice, how we handle your personal information or you would like to update the information we hold about you, please contact Helen Boothroyd: helen.boothroyd@placeforhope.org.uk.

If you are unhappy about how we processes your personal data, you can:

- submit a complaint to Georgia Boon: georgia.boon@placeforhope.org.uk; or
- notify the Information Commissioner's Office (ICO) by calling their helpline on: 0303 123 1113.