Data Protection Policy and Employee Privacy Notice

Introduction

Purpose

The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, 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, interns, apprentices] and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

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

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 – see Appendix. 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.

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.

The organisation will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment, or other type of contract, is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

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, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- 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, you should 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 him/her 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 the Administration and Finance Manager at 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 EU or UK law or where it is necessary to establish or defend legal claims.

Data security

The organisation takes the security of HR-related 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 in the proper performance of their duties. Electronic devices used to access data are password protected and passwords are only available to staff. 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 HR-related 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 HR-related personal data to countries outside the 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 moves house or changes his/her 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, volunteer period, internship or apprenticeship. 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 access to premises, 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;
- not to store personal data on local drives or on personal devices that are used for work purposes; 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 training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Retention Periods

The following timescale outlines the retention and disposal of all workers records:

a Recruitment Records – 6 months after the successful appointment

b Payroll, salary, benefit data – 7 years

c Maternity, paternity pay records – 3 years

d Criminal record checks – deleted promptly after the information has been verified

e Personal files – retained 7 years after the staff member has left the organisation

f Finance Records – retained 7 years

g Personnel Records – full personnel file – held for full duration of employment. Certain records held for a number of years after the staff member has left the organisation. 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.

After the above periods, both manual and electronic records shall be destroyed securely.

Policy review

This policy will be reviewed every two years.