NORTH EAST THAMES AREA QUAKER MEETING

Data protection policy – workforce

Introduction

This policy applies to the processing of personal data in manual and electronic records in relation to employment matters.

The Area Meeting is the Data Controller for the purposes of the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy applies to the personal data of job applicants, existing and former employees, volunteers, workers and self-employed contractors. These are referred to in this policy as 'relevant individuals'.

Definitions

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Commitment

As a responsible employer, we make a commitment to ensuring that personal data, including special categories of personal data and criminal offence data, is processed in line with GDPR and the Data Protection Act 2018. Where third parties (such as a payroll or pension provider) process data on our behalf, we will ensure that the third party takes such measures as are necessary to maintain our commitment to protecting data.

Types of data held

Personal data is kept in hard copy or in electronic form. The following types of data may be held on relevant individuals:

- name, address, phone numbers - for individual and next of kin

- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

Further information on the reasons for our processing activities, the lawful bases we rely on for the processing and data retention periods can be found in our workforce privacy notice and our job applicant privacy notice.

Data protection principles

All personal data obtained and held by us will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.

Personal data will be processed in recognition of an individuals' data protection rights and in accordance with the legal conditions for processing.

Procedures to protect personal data

The area meeting has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- We have appointed a Trustee with specific responsibility for data privacy.
- We provide information to relevant individuals on their data protection rights, how we use their personal data, and how we protect it. The information is contained in our workforce privacy notice and job applicant privacy notice.
- We ensure that those who may process data read and adhere to this policy.

- We analyse and can account for all personal data we hold, where it comes from, who it is shared with and also who it might be shared with.
- From the above analysis of data, we take measures to reduce the risks of mishandling and potential breaches of data security.
- We seek consent to process data on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
- We are aware of our duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner and we will ensure we do so.
- We are aware of the implications of international transfer of personal data (although we do not anticipate needing to do so).

Employee obligations in respect of protecting data

Employees and others who process data on our behalf will only have access to personal data where it is necessary for them to carry out their duties. These individuals must:

- ensure that all files or written information of a confidential nature are stored in a secure manner (eg in lockable cabinets or password-protected computers) and are only accessed by people who have a need and a right to access them;
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people;
- check regularly on the accuracy of data.

Access to data and subject access requests

Relevant individuals have a right to access the data that the area meeting holds about them. Requests for access to this data will be dealt with in accordance with the law and should be addressed to our Data Privacy Officer (details below).

Data disclosures

We may need to disclose/share certain data/information in some circumstances.

Our workforce privacy notice and job applicant privacy notice explain the circumstances in which data may be disclosed and to which organisations or individuals.

Disclosures will only be made when strictly necessary for the purpose.

International data transfers

We do not anticipate transferring personal data to any recipients outside of the EEA.

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the area meeting becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

Records and retention of data

We keep records of our processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

Generally, we will keep records until six years after individuals cease working, volunteering or providing services to us. After that time, we will only keep a record of name, capacity in which the individual worked or volunteered for us, the dates they did so and the reason for leaving. This is for the purposes of providing references and to deal with any other enquiries related to the engagement that may arise. It may also be for legal reasons, for example if there is a legal case in connection with the work or volunteering with.

Data protection compliance

Kate Green (Clerk to AM Trustees) is our appointed Data Privacy Officer in respect of its data protection activities. She may be contacted at 72 Nightingale Lane, London E11 2HE

May 2018