Data Protection Policy

Introduction

Purpose

The Trussell Trust 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, 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 charitable object purposes.

The Trussell Trust has appointed Emma Revie, CEO, as the person with responsibility for data protection compliance within the organisation. She can be contacted at emma.revie@trusselltrust.org. Questions about this policy, or requests for further information, should be directed to the **People & Culture (HR) data protection contact:**
Laura Mitchell, Director of People & Culture
laura.mitchell@trusselltrust.org
01722 580209
The Trussell Trust, Unit 9 Ashfield Road Trading Estate, Salisbury, SP2 7HL

Definitions

"**Personal data**" is any information that relates to an 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, biometric data, and criminal history, including actual and alleged offences (special conditions apply to the processing of such data).

Data protection principles

The Trussell Trust 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. It will not process personal data of individuals for other reasons.

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 provisions of Schedule 3 of the Data Protection Act (see below).

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, worker, or contractor relationship 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.

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).

Special categories of personal data

To lawfully process sensitive personal data, at least one of the conditions contained in Schedule 3 of the Data Protection Act must be met:

- explicit consent of the data subject has been freely given
- processing is necessary to comply with any obligation or legal duty imposed on the data controller
- processing is necessary to protect the vital interests of the data subject or another person (for example, life threatening issues such as disclosure of a data subject's medical history to a hospital casualty department treating the data subject after a road accident)
- processing is necessary for, or in connection with, legal proceedings (including prospective legal proceedings)
- processing is necessary for the exercising of legal rights or obtaining legal advice
- information contained in the personal data has been made public by the data subject for equal opportunities monitoring
- processing is necessary as it is deemed to be in the public interest.

The Trussell Trust processes special categories of personal data accordingly.

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 an individual makes a subject access request, the organisation will tell them:

- whether or not their 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 their 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 their personal data is stored (or how that period is decided)

- their rights to rectification or erasure of data, or to restrict or object to processing
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making

The organisation will also provide the individual with a copy of the personal data undergoing processing. This may be in electronic or paper format depending on the format of the request. If the individual wants additional copies, the organisation will charge a fee which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, please contact the People & Culture data protection contact (details are at the beginning of this document). In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires to do so.

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. The organisation will write to the individual within one month of receiving the original request to tell them 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, the organisation 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 the organisation has 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

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data
- stop processing or erase data that is no longer necessary for the purposes of processing
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data)
- stop processing or erase data if processing is unlawful
- stop processing data for a period if the data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps the individual should contact the People & Culture data protection contact, whose details are at the beginning of this document.

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. Restricted access to folders, password protection, and server security protects data kept in digital format; paper records are secured in locked filing cabinets in locked buildings to which access is limited to members of the People & Culture and finance teams.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality, and are obliged to implement appropriate technical and organisational measures to ensure the security of 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 to 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 their bank details.

Individuals may have access to the personal data of other individuals (including our partners and donors) in the course of their employment or contract. Where this is the case, the organisation relies on individuals to help meet its data protection obligations.

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)
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not to store personal data on local drives or on personal devices that are used for work purposes

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 personal 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.

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.