

Data Protection Policy

The Change Foundation

Introduction

Purpose

The charity is committed to being transparent about how it collects and uses personal data and to meeting its data protection obligations under the General Data Protection Regulation and other data protection legislation. This policy sets out the charity's commitment to data protection, and individual rights and obligations in relation to personal data.

The charity has appointed Carol Driver as its data protection officer. Her role is to inform and advise the organisation on its data protection obligations. She can be contacted at caroldriver@changefdn.org.uk. Questions about this policy, or requests for further information, should be directed to the data protection officer.

Definitions

"**Personal data**" is any information that relates to an individual who can be identified from that information and includes opinions about that person. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Data protection principles

The charity processes all personal data in accordance with the following data protection principles:

- The charity processes personal data lawfully, fairly and in a transparent manner.
- The charity documents what personal data it holds, where it came from and who we share it with. It then identifies and documents the lawful bases for processing them.
- When it is our legitimate business interest to hold data, we identify that interest.
- The charity reviews how it asks and records consent (when needed).
- The charity keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay. It has a process to recognise and respond to individual's requests to access and rectify their personal data and to objections.
- The charity keeps personal data only for the period necessary to meet the business interest and securely disposes of data no longer required.
- The charity 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 charity provides information notices to individuals on which we hold data.

- The charity regularly monitors its compliance with data protection policies and its data handling and security control.
- The charity has written contracts with organisations that process its data.
- The charity manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively
- Decision makers and key people in the charity demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the organisation
- The charity has an information security plan
- The charity has effective processes to identify, report, manage and resolve any personal data breaches
- The charity has an adequate level of protection for any personal data processed by others outside the European Economic Area.

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 charity will tell him/her:

- whether or not his/her data is processed
- description of the data and the reasons it is being processed and whether it will be given to any other organisations or people.
- The charity will also provide the individual with a copy of the personal data.
- Given details of the source of the data (where this is available)

To make a subject access request, the individual should send the request to caroldriver@change4dn.org.uk. In some cases, the charity may need to ask for proof of identification before the request can be processed. The charity will inform the individual if it needs to verify his/her identity and the documents it requires.

The charity 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 him/her 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 him/her 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.
- The charity will 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; and
- stop processing data for a period if 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 send a request to caroldriver@change4dn.org.uk or at The Change Foundation, Cricket Ground, Plough Lane, Wallington, Surrey SM5 8JQ

Data security

The organisation takes the security of personal data seriously. The organisation has 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.

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

Staff responsibilities

Staff are responsible for helping the organisation keep their personal data up to date. Staff should let the organisation know if data provided to the organisation changes, for example if you move to a new house or change your bank details. You should also ensure that the data we have on programme participants is as up to date as possible.

Staff will have access to the personal data of others in the course of their employment for example programme participants. Where this is the case, the organisation relies on staff to help meet its data protection obligations.

Staff 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.

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 programme participant data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal.

Training

The organisation will provide training to all staff about their data protection responsibilities as part of the induction process.

Staff 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.

Information notice for The Change Foundation staff

The Change Foundation works hard to make sure that we look after and protect all personal data that we hold on our staff. The Change Foundation is registered with the Information Commissioner as a registered data controller.

This information notice outlines what you can expect when the charity collects your information. The legal basis we hold information is called legitimate business interest. The charity will only use information for its legitimate business interests which are to pay you, be in contractual relationship with you regarding your work , provide other staff benefits , manage performance and the wider work to achieve and promote the charity's activities, mission and objectives . We also have a legal requirement to collect tax information for the Inland Revenue.

What information do we collect about you?

In order to carry out its duties as an employer, the charity must collect and process data relating to its staff.

A record relating to your employment will be held by the charity mainly in your personal file which is paper based and more limited information in electronic form. Information

about your employment may also be held by individual managers.

Data held about you may include, but is not restricted to, the following:

Application forms

Personal details such as name, date of birth, telephone number and email address, contact and next-of-kin details, and National Insurance number

Visa details and copies of passports

Bank or building society account details

Salary and grade details, including data held on staff organisational charts

Superannuation details

Records concerning appraisal and training

Sickness and other absence details

Proceedings relating to promotions

Contracts or terms and conditions, of employment

Correspondence between the member of staff and the charity

Correspondence, such as references, between charity and third parties on behalf of a member of staff

CCTV records

Records of grievances

Investigations into breaches of terms and conditions of employment

Records of disciplinary proceedings

Health and safety records (including accident reports)

Timesheets and expenses

Photographs

Audio and/or video recording of staff giving coaching or in workshops

How will we use information about you?

The Charity processes staff personal data in order to

Pay your salary into your bank account and make pension contributions

Organise staff benefits

Review staff performance

Assess suitability for promotion

Monitor absence and sickness records in accordance with charity policy

Enable staff to undertake their roles in coaching
Publish the print and online staff directories of basic contact details
Monitor the performance of the charity e.g. Time sheets
Arrange travel and other activities
Other necessary organisational tasks such as emergency contact procedures

Who has access to your data?

Where data is held in your personal file access to personal files is carefully controlled and they may only be seen by the Charity Administrator, the Corporate Services Director, Head of Finance, your Manager, the Chief Executive, auditors and other persons, if authorised by the Corporate Services Director.

Sensitive personal data

The Charity recognises the significance of sensitive personal data and will only process such data if certain conditions are met. These conditions are outlined in guidance from the UK Information Commissioner's Office. We ask you to declare your ethnic origin, and any disabilities at the time of your application for a post. These fall within the definition of sensitive data. If you choose to provide such data, you give your consent for the charity to use them, in aggregated form, for statistical purposes. Your HR file may also contain sensitive personal data in relation to health or sickness, criminal record, your gender and sexual orientation, maternity leave or paternity leave. These records will be kept in strict confidence and will not be released to third parties without your explicit consent.

Sharing and disclosing your personal information

The Charity may disclose certain personal data to external bodies as categorised below. At all times, the amount of information disclosed and the way it is disclosed will be in the legitimate business interests of the charity. Please note this is not an exhaustive list.

Who we may share information with:

Disclosure and Barring Service (DBS) Required for certain sensitive posts to assess applicant's suitability for positions of trust. Mortgage lender and letting agencies. In order to allow these organisations to verify for mortgages and tenancy agreements. Release of this information is subject to written consent from the employee. UK agencies with duties relating to the prevention and detection of crime, apprehension and prosecution of offender, collection of a tax or duty, or safeguarding national security* As necessary, and with appropriate consideration of your rights and freedoms (such as Benefit or Tax Inspectors, the Police, UK Visas and Immigration,

or the Foreign and Commonwealth Office).* such as the Department of Work & Pensions, Police, UK Visas and Immigration, or the Foreign and Commonwealth Office.HM Revenues & Customs (HMRC)Real Time Information released to HM Revenue & Customs (HMRC) in order to collect Income Tax and National Insurance contributions (NICs) from employees.

Pension scheme data required for the provision of pensions by Aegon. Insurance provider the provider of the critical illness policy and death in service benefits . Business continuity purposes

Third party software suppliers

Where external computer systems are required to facilitate the purposes listed above e.g. Payroll, pension staff data may be shared with software suppliers. Any such transfer will be subject to a formal agreement between the charity and those suppliers, to ensure protection of your personal data.

Retention periods

Within 6 months of staff leaving the charity information in the staff file is reduced to that required to respond to reference requests and any historic child abuse claim that may arise.

Requesting information

You may at any time request to see the information that we hold on you to do this you must write or email to the contact details given here. office@changeofdn.org.uk our address is The Change Foundation, Plough Lane, Wallington, Surrey SM6 8 JQ. The Data Protection Officer is Carol Driver. Further concerns can be raised with the Information Commissioner. www.ico.org.uk