EMPLOYEE DATA PROTECTION & PRIVACY POLICY

Introduction

Durham Community Action, whose registered address is at 8 St Stephen's Court, Low Willington, Co. Durham DL15 0BF is a 'data controller'. This statement explains why and how we collect & process data about our employees, and how we ensure that the privacy of that data is protected. We are permitted to hold and process data about you because you are an existing / prospective employee and there is an existing / potential contract between us, which provides the legal basis for processing the information. Please note that the policy does not confer any contractual rights.

Our obligations

We must comply with the following obligations when we process any of your personal data:

- Ensuring that the data we collect is accurate and up to date.
- Using your data in a way that is fair, transparent, and lawful.
- Only collecting data for valid and relevant reasons that we have explained to you and limiting its use for those reasons. If we need to use your personal data for a different and unrelated purpose, we will write to explain the legal basis for doing so.
- Ensuring that your data is kept securely in a format that only identifies you for as long as deemed necessary.

In exceptional circumstances we may have to use your personal data without your knowledge or consent where this is required by law.

We will make every effort to only ask for data that supports the contractual employment relationship or any associated legal obligations. If you choose not to provide the data, we may not be able to fulfil our contractual or legal obligations to you.

For Durham Community Action to meet the obligations of managing your contract or to meet legal obligations connected with your employment relationship, it is necessary to share your personal information with certain third parties (e.g., pension provider, legal or professional advisers). Durham Community Action may also share your personal data with other third parties (e.g., through Transfer of Undertakings Protection of Employment). Durham Community Action does not transfer personal data outside the EEA.

Individual rights and obligations

Current data protection legislation provides the following rights for individuals:

- The right to be informed.
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing.
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

In order that we can ensure that the personal data we hold in relation to you is accurate, it is important that you keep us informed of any changes to your data.

What data might we collect?
We collect a wide range of data (as detailed below), beginning with the application process, and references from current or former employers. Where any additional personal data is needed, we will ask you for this in writing, setting out the purpose for which is it required.

a. Recruitment data
We collect information about previous employers and jobs, skills, and qualifications, to help us make decisions regarding your suitability for employment/engagement. Data obtained during the recruitment process will be retained for six months after an application has been declined to answer any queries that may arise. If you are appointed, your data will be kept for the duration of your employment and for 12 months afterwards.

b. Right to work.
We may ask to see a copy of your passport, visa, or work permit as evidence of your right to work in the UK. This data will be kept for the duration of your employment and for two years afterwards.

c. Personnel data
We will collect key personal data about you: e.g., name address, telephone / mobile numbers, e-mail address, date of birth, next of kin, etc. This will allow us to send you any correspondence and will tell us who to contact in an emergency. This data will be kept electronically on Sage Payroll, and in paper format in a secure file, for the duration of your employment and for 12 months afterwards.

d. Payroll data
We will collect and retain bank details, salary history, details of benefits, tax, national insurance and NI number, tax status, pension contributions, other deductions, student loans etc. This will enable us to pay you correctly and to fulfil our reporting obligations to HMRC. We will retain this information in secure electronic and paper.
forms for 6 years after last update, in accordance with HMRC regulations.

e. Timesheets and leave records.
We will retain timesheets to ensure that you are working the correct hours and receiving the correct leave, and that our obligations under the Working Time Regulations are being met. We will retain this data for the duration of your employment and for 12 months afterwards.

f. Health and medical records
With your consent, we may hold information about your health and medical conditions, including self-certification, GP fit notes, and any report from your GP, consultant, or an occupational health specialist. This information will help us to assess your ability to undertake your role, or alternative roles, and to make any workplace adjustments to improve your working environment. The data will normally be kept for the duration of your employment and for 12 months afterwards, although if it relates to an accident at work, we will retain the data for 4 years after your employment ends.

g. Ethnic monitoring data
We may collect data related to your racial origin, to understand the diversity of our workforce, and for rebalancing purposes if we believe we do not have the correct diversity. This data will be kept for the duration of your employment and for 12 months afterwards.

h. Disciplinary and grievance data
We will hold this data for the duration of your employment and for 12 months afterwards for monitoring and reference purposes. Warnings will be 'live' for the duration specified in them.

i. Other data
We will collect and retain other data, including start date, workplace, flexible working requests, training records, professional memberships, job performance details, appraisals, supervision notes, photographs, use of IT/ communication systems etc. This information may be used to calculate entitlements to benefits linked to length of service, understand your work performance, assess training needs, ensure policy compliance, make decisions about promotion or continued employment, and for promotional purposes e.g., website entries. This data will be kept for the duration of your employment and for 12 months afterwards.

j. Third parties
If you enrol in our pension scheme, we will need to share certain data with The Pensions Trust to allow them to process your benefits. This data will be kept for the duration of your employment and for 12 months afterwards, although the pension provider may need to keep this data longer to fulfil their obligations to you.

k. Reference data
We may need to retain basic information e.g., name, address, start and leave dates, job history, last salary details, training etc. in order to fulfil reference requests from prospective employers. We will normally retain this data for up to five years after your leave our employment, although references provided for ex-employees will normally be kept for 12 months and then destroyed.

l. Contracts
Occasionally we may need to retain employee data for a longer period to comply with our contractual obligations to funders. In such circumstances, the requirements of funders will take precedence over DCA's own document retention policies.

When will we use your personal / special category data?
We will normally use your personal data to comply with legal obligations, fulfil our contractual obligations to you, or where it is necessary for legitimate interests (including those of a third party). Occasionally we may need to use your personal data or special category data to protect your interests (or someone else's interests), in the public interest, where it has already been made public, or where it is needed for legal claims.

Special category data e.g., identifying ethnic origin, details of disabilities etc may be used to comply with employment and other laws, health and safety, or where it is needed in the public interest, for example for equal opportunity monitoring and reporting. In limited circumstances, Durham Community Action may request your written consent to allow us to process special category data. Durham Community Action will only collect data about criminal convictions if it is deemed appropriate to the role and duties you will perform.

Subject Access Requests
You are entitled to make a subject access request (SAR) by writing to the Executive Director. If you make an SAR, we may request specific information to confirm your identity, so as to ensure that the data is released to the correct person. The information will be provided in a commonly used electronic form, unless otherwise requested by the individual. We will only charge you a fee for an SAR if your request is 'manifestly unfounded or excessive', or if further copies of data are requested.

We will normally respond to an SAR within 30 calendar days, although this deadline may be extended for particularly complex requests. We may withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others.

Data breaches

Where any personal data is lost, destroyed, corrupted, or disclosed etc. this will amount to a data breach. In such circumstances, staff must immediately inform their line manager. We will investigate the cause of any breach, determine any remedial action that can be taken and consider how the effect of the breach can be mitigated. Our initial priority will be to contain the breach, and to assess the potential adverse consequences for the individual(s) concerned.

If personal data has been sent to someone who is not authorised to have access to it, we will:

- Inform the unauthorised recipient not to distribute it in any way or discuss it with anyone else.
- Inform the unauthorised recipient to destroy or delete the data.
- Request the unauthorised recipient to confirm in writing that they have destroyed/ deleted the data.
- Advise the unauthorised recipient of the implications if they disclose the data.
- If relevant, inform the data subject(s) so that they can take any necessary action.

When a personal data breach has occurred, we will need to establish the likelihood and severity of the risk to individual(s) rights. If there is a risk, we will notify the Information Commissioners Office (ICO). If we consider any risks to be unlikely, we will not be required to report to the ICO. Notifiable breaches must be reported to the ICO no later than 72 hours after we first become aware of them.

Last updated - February 2021