|  |
| --- |
| **Positive Support for You CIC**  **Employee Data Protection Policy**  **May 2018** |

****

Version. 1/ 05/2018

# Introduction

This Policy sets out the obligations of the Company with regard to data protection and the rights of employees in respect of their personal data under the Data Protection Act 1998 (“the Act”) and as amended by the General Data Protection Regulation (GDPR) coming into force on the 18 May 2018.

This Policy sets out the procedures that are to be followed when dealing with personal data and apply to employees of the Company, contractors, or third parties working on behalf of the Company.

The Company is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all employees.

Employee data is collected by the Company in order to ensure that the Company can effectively and efficiently manage its employees, comply with its legal obligations, and create a fair, equal and anti-discriminatory workplace.

# Data Protection Principles

## Employee data will be processed fairly and lawfully.

The data held is necessary for the purposes of legitimate interests pursued by the Company or by a third party to whom the data is disclosed.

The processing of this data is necessary for the performance of the employment contract and for compliance with any legal obligation to which the Company is bound.

Where information about the Employee is considered to be “sensitive” the employee will be asked for specific consent for the Company to hold that information unless:

* it is necessary for exercising any right or obligation imposed by law on the Company in connection with employment.
* it is necessary for the purpose of, or in connection with, any actual or prospective legal proceedings.
* it is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
* It is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, or any other protected characteristic, with a view to enabling such equality to be promoted or maintained.

## Employee data will be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes.

Employees will be provided with a Privacy Notice that details what data the company holds about them and their rights with regards to this information.

The data collected will be relevant and not excessive for the purpose. It will be held accurately and updated as necessary and will not be used for any purpose that is incompatible with employment.

All Employee data will be held for only as long as necessary and will be securely destroyed after.

Any information that relates to an actual or potential claim against the Company, or for any other legally specified period, will be held indefinitely.

Employee data will not be transferred outside of the European Economic Area.

Proportionate measures will be taken by the Company to protect employee data against unauthorised or unlawful processing, accidental loss, destruction or damage.

# Rights of Employees

Employees have the following rights:

* The right to access a copy of their personal data held by the Company by means of a Subject Access Request.
* The right to object to any processing of their personal data that is likely to cause damage or distress. Employees should make any such objection in writing to their Manager. The Company will respond within 28 days. However, it should be noted that the Company may not comply with your request if it is considered unjustified.
* The right to have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances.
* The right to claim compensation for damage caused by the Company’s breach of the Act.

# Personal Data

Personal data is defined as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the Employer. This includes any expression of opinion about the individual and any indication of the intentions of the Employer or any other person in respect of the individual.

The Act also defines “sensitive personal data” as that relating to the racial or ethnic origin of the Employee; their political opinions; religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; details of actual or alleged offences.

The Company only holds personal data that is directly relevant to its employees. That data will be collected, held and processed in accordance with the data protection principles and with this Policy.

The following data may be collected, held and processed by the Company:

* Identification information relating to employees including, but not limited to, names, contact details, age, emergency contacts and right to work documentation.
* Details collected and submitted to the Discolusure and Barring Service.
* Bank details and personal data necessary to process payroll, pensions and other benefits. This includes any deductions required by law, or as requested by employees, such as trade union deductions or health schemes.
* Equal opportunities monitoring information including age, gender, sexual orientation, race, nationality, pregnancy, disability and religion.
* Health records including details of sick leave, medical conditions, disabilities and prescribed medication, for the purpose of managing and monitoring the capabilities of employees. The Company is committed to maintaining health and safety in the workplace and in promoting equal opportunities and preventing discrimination on the grounds of disability or other medical conditions.
* Employment records including, but not limited to, interview notes, curricula vitae, application forms, review of social media profiles, references, assessments, performance reviews and similar documents.
* Details of salaries and benefits including increases, bonuses, commission, overtime, benefits and expenses.
* Records of disciplinary matters including reports and warnings, both formal and informal.
* Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes.
* Absence records for monitoring attendance and entitlements
* CCTV footage for security purposes
* Vehicle tracking systems for operational and performance purposes
* Records of all processing undertaken on work computers and other technology, including personal email accounts.
* Training Records

# Security of data

All data is held securely by the Company and access is only permitted for legitimate purposes, such as

* Review of historical matters for contractual, legal or operational reasons
* Amendments to terms and conditions of employment
* Disciplinary or grievance matters
* Review of flexible working requests, maternity and other absence
* Equal opportunity monitoring

In general terms those with legitimate access are the Line Manager, their Manager and other Senior Managers, third parties such as payroll and HR. Others may be given access in specific prescribed situations, such as when undertaking a disciplinary investigation or seeking legal advice.

Under no circumstances will personal data be passed to any department or any individual within the Company, or externally, that does not reasonably require access to that personal data in view of the purpose(s) for which it was collected and is being processed.

Reasonable efforts will be made to get consent from an Employee before any sensitive personal information is shared more widely, such as in circumstances when an Employee is absent form work.

Employees have the right to request that the Company does not keep health records on them. All such requests must be made in writing and addressed to the Line Manager.

# Monitoring

The Company may from time to time monitor the activities of employees. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring, vehicle tracking and CCTV. Monitoring takes place to

* Assess usage and functionality
* To allow investigation of individuals where wrongdoing is suspected
* To inform decisions within the business

Monitoring will only take place if the Company considers that it is necessary to achieve the benefit it is intended to achieve. Data collected during any such monitoring will only be collected, held and processed for reasons directly related to (and necessary for) achieving the intended result.

The Company will use reasonable endeavours to ensure that there is no intrusion upon employees’ personal communications or activities and under no circumstances will monitoring take place outside of the employee’s normal place of work or work hours unless the employee in question is using Company equipment or other facilities outside of working hours, or premises.

# Data Protection Procedures

The Company shall ensure that all of its employees, agents, contractors, or other parties working on behalf of the Company comply with the following when working with personal data:

* All emails containing personal data will, whenever practical, be encrypted or password protected.
* Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
* Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.
* Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient if practical or sent using guaranteed delivery Royal Mail.
* No personal data will be shared informally.
* All hardcopies of personal data, along with any electronic copies stored on physical, removable media will be stored securely.
* Personal data will be handled with care at all times and will not be left unattended or on view to unauthorised parties.
* If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
* Any unwanted copies of personal data that are no longer needed will be disposed of securely. Hardcopies should be shredded and electronic copies should be deleted securely.
* No personal data should be routinely stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), unless it is a Company device, used only for Company purposes and is secured by password. It should be removed from a mobile device as soon as practical.
* No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to third parties working on behalf of the Company where they have agreed to comply with this Policy and of the Act.
* All personal data stored electronically should be backed up daily with backups stored securely offsite or in secured cloud storage.
* All electronic copies of personal data should be stored securely using passwords where practical.
* All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised.
* Under no circumstances should any passwords be shared between employees or third parties with the admin officer who will hold securely details of all passwords for use in emergency circumstances.

# Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

* The Company has appointed the Chief Executive will act as Data Protection Officer with the specific responsibility of overseeing data protection and ensuring compliance with this Policy and with the Act. The Data Protection Officer shall in particular be responsible for:
  + Overseeing the implementation of, and compliance with this Policy, working in conjunction with the relevant employees, managers and/or department heads, agents, contractors and other parties working on behalf of the Company.
  + Keeping up to date with legal and technological changes relating to data protection
  + Reviewing this Policy and all related procedures not less than annually.
* All employees or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company’s responsibilities under the Act and under this Policy.
* Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
* The performance of those employees or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

# Access to Personal Data

An Employee may make a subject access request (“SAR”) at any time to find out more about the information which the Company holds about them.

SARs should be made in writing, addressed to the Chief Executive and specify clearly what data is required and for what time period..

Upon receipt of a SAR the Company shall have a maximum period of 28 calendar days within which to respond fully.

# Employee Records and Retention

The Company shall retain all employee records following the end of employment for the following periods:

|  |  |
| --- | --- |
| Staff files including training and appraisal records | 10 years |
| Payroll, pensions, benefits data  Sickness and health data | 10 years  indefinitely |

Any statutory requirement will take precedent over these time periods

Any documents that may be required for legal reasons, such as Employment Tribunals or other court cases will be held indefinitely.

# Implementation of Policy

This Policy is effective as of 21st May 2018.

This Policy has been approved & authorised by Board of Directors:

|  |  |  |
| --- | --- | --- |
| **Review Date** | **Name** | **Signed** |
| 21/05/2018 | Dave Barras | DAVE SIG.jpg |