The Wild Hub CIC

DATA PROTECTION POLICY

Introduction

The CIC is committed to being transparent about how it collects and uses personal data and to meeting its data protection obligations. This policy sets out the CIC's commitment to data protection as well as individual rights and obligations.

As a not for profit organisation, we are exempt from registering with the ICO but follow the data protection principles laid down under the Data Protection Acts and GDPR.

This policy applies to the personal data of job applicants, employees and contractors and former employees, referred to as HR-related personal data.

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 and biometric data.
- **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The CIC processes HR-related personal data in accordance with the following data protection principles:

- personal data is processed lawfully, fairly and in a transparent manner.
- personal data is collected only for specified, explicit and legitimate purposes.
- personal data is processed only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- accurate personal data will be kept and all reasonable steps taken to ensure that inaccurate personal data is rectified or deleted without delay.
- personal data is kept only for the period necessary for processing.
- appropriate measures will be adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

The CIC will advise the reasons for processing personal data, how they use such data and the legal basis for processing it in privacy information notices (PINs). The CIC will not process personal data for any other reason.

Where the CIC 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 a policy on special categories of data and criminal records data.

The CIC will update HR-related personal data promptly if an individual advises us that their information has changed or is inaccurate.

Personal data gathered during the employment or contractor relationship is held in the individual's personnel file in electronic format and on HR systems, as appropriate. The periods for which the CIC may hold HR-related personal data are detailed in the privacy information notice.

A record of our processing activities for any HR-related personal data is held in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

If an individual wants to make a subject access request, the CIC will tell them:

- whether or not their personal 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 right 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 CIC has failed to comply with data protection rights; and
- whether or not the CIC carries out automated decision-making and the logic involved in any such decision-making.

The CIC will also provide a copy of the personal data undergoing processing. This will normally be in electronic form if the request has been made electronically, unless agreed otherwise. If additional copies are required, the CIC may charge a fee, which will be based on the administrative cost of providing additional copies.

A subject access request should be sent to the Chair. In some cases, proof of identification may be required. The CIC will normally respond to a request within a one month from the date it is received.

If a subject access request is manifestly unfounded or excessive, the CIC is not obliged to comply with it, we will notify individuals accordingly. Alternatively, it can agree to respond but will charge a fee.

Other rights

These may be asking the CIC 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 an individual's interests override our legitimate grounds for processing data (where the CIC relies on our 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 their individuals' interests override our legitimate grounds for processing data.

To take any of these steps, requests should be sent to the Chair.

Data security

The CIC takes the security of HR-related personal data seriously. Internal policies and controls are 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 CIC engages third parties to process personal data on the CIC's 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 CIC discovers that there has been a breach of HR-related personal data that poses a risk to individuals rights and freedoms this will be reported to the Information Commissioner within 72 hours of discovery. All data breaches will be recorded regardless of their effect.

If the breach is likely to result in a high risk to rights and freedoms, the CIC will tell individuals and provide information about its likely consequences and the mitigation measures taken.

International data transfers

The CIC will not transfer HR-related personal data to countries outside the EEA.

Individuals' responsibilities

Individuals are responsible for helping the CIC keep their personal data up to date. They should let the CIC know if their personal data changes, e.g., move house, change bank details, etc.

Individual's may have access to the personal data of others, of customers and suppliers in the course of employment. Individuals 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 CIC) 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 our premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that is used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the CIC's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The CIC will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

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.