DATA PROTECTION POLICY

1. Introduction

This document sets out the obligations of the Zennistoun Hub C.I.C.("the Company") with regard to data protection and the rights of people with whom it works in respect of their personal data under the General Data Protection Regulations (GDPR, 2018) ("the Act").

This Policy shall set out procedures which are to be followed when dealing with personal data. The procedures set out herein must be followed by the Company, its volunteers, employees, contractors, agents, consultants, partners or other parties working on behalf of the Company.

The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Company shall ensure that it handles all personal data correctly and lawfully.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out eight principles with which any party handling personal data must comply.

All personal data:

2.1 Must be processed fairly and lawfully (and shall not be processed unless certain conditions are met);

2.2 Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes;

2.3 Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;

2.4 Must be accurate and, where appropriate, kept up-to-date;

2.5 Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed;

2.6 Must be processed in accordance with the rights of data subjects under the Act;

2.7 Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and

2.8 Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Rights of Data Subjects

Under the Act, data subjects have the following rights:

- The right to be informed that their personal data is being processed;
- The right to access any of their personal data held by the Company within 40 days of making a request;
- The right to prevent the processing of their personal data in limited circumstances; and
- The right to rectify, block, erase or destroy incorrect personal data.

4. Personal Data

Personal data is defined by the Act 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 data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Act also defines "sensitive personal data" as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The Company only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the data protection principles and with this Policy.

5. Processing Personal Data

Any and all personal data collected by the Company (including that detailed in Section 4 of this Policy) is collected in order to ensure that the Company can facilitate efficient transactions with third parties including, but not limited to, its customers, partners, associates and affiliates and efficiently manage its volunteers, employees, contractors, agents and consultants. Personal data shall also be used by the Company in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within the Company. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any

individual within the Company that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

The Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully;
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s);
- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed;
- No personal data is held for any longer than necessary in light of the stated purpose(s);
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred using secure means, electronically or otherwise;
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory; and
- All data subjects can exercise their rights set out above in Section 3 and more fully in the Act.

6. Data Protection Procedures

The Company shall ensure that all of its volunteers, employees, contractors, agents, consultants, partners or other parties working on behalf of the Company comply with the following when processing and / or transmitting personal data:

- All emails containing personal data must be encrypted;
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- 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. Using an intermediary is not permitted;

- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar;
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet; and
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.

7. Organisational Measures

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

- A designated officer ("the Designated Officer") within the Company shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act.
- All volunteers, employees, contractors, agents, consultants, partners 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 shall be furnished with a copy of this Policy.
- All volunteers, employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
- All volunteers, employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The Performance of those volunteers, employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
- All volunteers, employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Act.
- All contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data must ensure that any and all of their volunteer or employees who are involved in the processing of personal data are held to the same conditions as those relevant volunteers or employees of the Company arising

out of this Policy and the Act.

- Where any contractor, agent, consultant, partner or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

8. Access by Data Subjects

A data subject may make a Subject Access Request ("SAR") at any time to see the information which the Company holds about them.

- SARs must be made in writing, accompanied by the correct fee.
- The Company currently requires a fee of £10 (the statutory maximum) with all SARs. [A fee of £2 shall be required for access to a credit file.]

Upon receipt of a SAR the Company shall have a maximum period of 40 days within which to respond. The following information will be provided to the data subject:

- Whether or not the Company holds any personal data on the data subject;
- A description of any personal data held on the data subject;
- Details of what that personal data is used for;
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.

9. Notification to the Information Commissioner's Office

As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. The Company is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Designated Officer shall be responsible for notifying and updating the Information Commissioner's Office.

10. Implementation of Policy

This Policy shall be deemed effective as of April 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved & authorised by:

Name:
Position:
Date:
Signature: