1.1 ICT DATA PROTECTION POLICY WITH GDPR

The purpose of this policy is to ensure that the company meets its obligations under The Data Protection Act 2018 and associated legislation, hereafter referred to collectively as 'DPA'. DPA requires data controllers (people or organisations that process data on living individuals) to comply with the Eight Data Protection Principles (the "Principles") governing the use of personal data laid down in DPA and to safeguard the privacy of individuals when processing their details.

Any employee deliberately or negligently acting outside their recognised authority will be subject to The Company's disciplinary procedures, including dismissal where appropriate, and may be subject to criminal proceedings. Data protection is a specialist area and employees should seek advice from the Data Protection Officer rather than risk exposing both themselves and The Company to criticism and possibly legal sanction.

Individuals whose information is held and processed by The Company can be assured that our policy is to handle their data in accordance with DPA. Other legislation may exceptionally override DPA - for example in the investigation of crime - and it should be noted that The Company intends to fulfil all of its legal obligations and responsibilities.

In terms of the Data Protection Act 2018, we are the 'data controller', and as such determine the purpose for which, and the manner in which, any personal data are, or are to be, processed. We must ensure that we have:

1. Fairly and lawfully processed personal data

Individuals will be informed of the purposes of the processing and the likely classes of recipients of such information; both internal and external. Forms used for collecting personal information will, where appropriate, give details of the purposes for which the information is required.

If a person feels they have been deceived or misled, they are entitled to make a complaint to the company.

2. Processed for a limited purpose

We will not use data for a purpose other than those agreed by data subjects (voluntary and community group members, staff and others). If the data held by us are requested by external organisations for any reason, this will only be passed if data subjects (voluntary and community group members, staff and others) agree. Also, external organisations must state the purpose of processing, agree not to copy the data for further use and sign a contract agreeing to abide by The Data Protection Act 2018 and (your name here) Data Protection Policy.

3. Adequate, relevant and not excessive

The company will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed.

4. Accurate and up-to-date

The Company will ensure, as far as is practicable, that the information it holds is accurate and, where necessary, up to date. When a person informs The Company of a change or an inaccuracy, the personal information will be amended, subject to satisfactory proof, as soon as reasonably possible.

5. Data Integrity – Retention

The Company will not hold personal information for longer than is necessary for the relevant purpose(s) for which that information was obtained. Where details are stored for long-term archive or historical reasons then, wherever reasonably possible, personal details will be removed, if required by DPA, so that individuals cannot be identified.

6. Subject Access Requests

The Company will process all requests from individuals for access to the personal data held on them ("subject access requests") within 30 calendar days as prescribed under DPA provided the requests are made in the form required. The Company reserves the right to seek confirmation of the identity of the person making the request and to ask for more details to help locate the data being requested. The countdown for the time limit for responses will not start until The Company has enough information to locate the data being requested and are satisfied as to the identity of the requester. Anyone receiving something that appears to be a subject access request should pass it to the Data Protection Officer immediately.

7. Secure

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. Obtaining ISO 27001 reflects this.

8. Not transferred to countries outside the European Economic Area, unless the country has adequate protection for the individual.

Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual. The Company takes particular care to be aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a website that can be accessed from outside the European Economic Area.

Edocuments Limited, Unit 32 Waterhouse Business Centre,
Chelmsford, Essex, CM1 2QE
Company Number: 04236508

www.edocuments.co.uk
info@edocuments.co.uk
T: +44 (0)1245 330010