ICO Ref: COM0571033

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Community Transport (Brighton,Hove & Area) Ltd

Preston Barracks
Lewes Road
Brighton
BN2 4GL

I, Edward Bassford, General Manager of Community Transport Ltd, for and on behalf of Community Transport Ltd hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Community Transport Ltd is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by Community Transport Ltd and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed on 12 February 2015 that a removable hard drive containing personal data had been taken home by a member of staff and that the individual concerned had subsequently failed to return it. The removable hard drive contained a back-up of Community Transport Ltd's customer database, which contained 4,138 individual records. This included some limited medical data. The standard procedure at Community Transport Ltd at the time of the incident was for a member of staff to take the back-up tape home each day so that it could be stored offsite. On this occasion, the member of staff tasked with taking the back-up tape home unexpectedly failed to return to work.

3. The Commissioner's enquiries have determined that the data controller could have taken steps to reduce the likelihood of an incident of this nature occurring. In particular, the Commissioner's investigation determined that guidance could have been offered to staff in three key areas as follows: by

offering regular, mandatory data protection training; by creating a formal procedure for staff to follow when taking personal data off-site and by having a robust policy to govern access and storage of personal data in place.

4. The Commissioner's investigation also revealed that the data controller was retaining data for longer than is necessary for its work, and that a procedure or policy to address this was lacking.

5. Finally, the Commissioner's investigation also revealed that data stored electronically on portable devices was not routinely encrypted before being moved off-site.

6. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Fifth and Seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

7. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Fifth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

(1) Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software which meets the current standard or equivalent;

(2) Policies relevant to the storage and use of personal data are improved in light of this incident;

(3) Policies and procedures relevant to the retention of personal data are implemented in light of this incident;

(4) Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;

(5) Staff responsible for the handling of personal data are given appropriate, specific training upon induction and this training is refreshed regularly;

(6) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: ……

Edward Bassford
General Manager
Community Transport (Brighton,Hove & Area) Ltd

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….