ICO Ref: **ENF0423165**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Enable Scotland (Leading the Way)

2nd Floor
146 Argyle Street
Glasgow
G2 8BL

I, Peter Scott, Chief Executive of Enable Scotland (Leading the Way) (the "charity"), for and on behalf of the charity, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Enable Scotland (Leading the Way) 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 the charity, 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 provided with a report in November 2011 about the theft of electronic equipment and hard copy documents from an employee's home. The electronic equipment consisted of a laptop and two memory sticks. The laptop, which did not contain any personal data, was password protected and had third party supplier software installed allowing its usage to be tracked. No usage has been logged since the theft.

3. The information stored on the two stolen memory sticks and within the accompanying work papers included limited sensitive personal data relating to up to 101 individuals. The data on the memory sticks was held for migration purposes. This was against policy as the details should only have been held on a temporary basis until they could be uploaded to a server. Investigations revealed that neither of the memory sticks were encrypted and that at the time of the incident, encryption of removable media devices was not mandatory. Moreover, there was no specific policy in place to cover

working away from the office.

4. In deciding what action to take, the Commissioner has considered that only limited, and in some cases abbreviated, sensitive personal data was involved for each individual and there is no evidence to suggest that the information in question has been inappropriately accessed. Although there were some gaps in procedure at the time of the incident, immediate and comprehensive remedial action was taken, and the use of all removable media devices is now prohibited.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data stolen 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.

6. 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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. Laptops 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 by no later than 16 March 2012;

2. Hard copy documentation is only removed from the office when absolutely necessary. It will contain the minimum amount of personal data required for its purpose and will be anonymised where possible;

3. A specific policy is put in place to cover working away from the office. This should include provisions on the handling of both electronic and hard copy personal data;

4. Staff are aware of the data controller's policies for the retention, storage and use of personal data and are appropriately trained how to follow those policies;

5. 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.

Dated…….

Signed……

Peter Scott
Chief Executive
Enable Scotland (Leading the Way)

Signed……

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