DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Stockport NHS Foundation Trust
Oak House
Stepping Hill Hospital
Poplar Grove
Stockport SK2 7JE

I, Dr Chris Burke, Chief Executive of Stockport NHS Foundation Trust (the Trust), for and on behalf of the Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Stockport NHS Foundation Trust 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 Trust 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 from Dr Chris Burke acting on behalf of the data controller, regarding the theft of a laptop computer which held the personal data of patients of the data controller.

3. The laptop computer was stolen from a locked room in the Stoma Care Offices, Willow House, Stepping Hill Hospital. The laptop held clinical information relating to 1588 patients which was password protected but not encrypted. The laptop was not locked in a cabinet as usual but due to refurbishment work being carried out was stored in a covered box under a desk. The laptop was provided and installed by a private company before the Trust's network facility was available and does not appear to have been registered with the Trust's IT department. Patient information appears to have continued being entered into a database on the laptop's hard drive after Network facilities became available.

4. 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 1 of 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.

5. 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 or from other data controllers in similar circumstances, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part 1 of 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) All computers and portable devices used by the data controller to process personal data are registered with the IT department;

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

(4) That adequate alternative data security arrangements are implemented when normal working practices cannot be followed:

(5) The data controller shall implement such other security measures it deems appropriate to ensure that personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage.

Dated..... 25th March 09

Signed.....
Dr Chris Burke
Chief Executive
Stockport NHS Foundation Trust

Signed..
Mick Gorrill 1/4/09 .
Assistant Commissioner Regulatory Action Division
For and on behalf of the Information Commissioner