[redacted]

5/7/10

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Birmingham Children's Hospital NHS Foundation Trust

Steelhouse Lane
Birmingham
B4 6NH

I, Sarah-Jane Marsh, Chief Executive, of Birmingham Children's Hospital NHS Foundation Trust, Steelhouse Lane, Birmingham, B4 6NH, for and on behalf of Birmingham Children's Hospital NHS Foundation Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Birmingham Children's Hospital 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 Birmingham Children's Hospital NHS Foundation 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 initially informed of a self reported security breach by the data controller on 5 March 2010. After further investigations by the data controller a draft investigation report was provided to the Commissioner on 8 June 2010.

3. On 1 March 2010 two unencrypted laptops belonging to Respiratory Medicine were stolen from the Medical Day Centre. The laptops were used as part of the diagnostic and on-going assessment of patients with sleep disordered breathing. Personal data including sensitive personal data relating to 17 patients was stored on the laptops and included patient diagnoses, the reason for each patient test and consultant and video recordings.

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 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.

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, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part 1 of schedule 1 to the Act, and in particular that:

(1) Adequate measures are put in place to ensure that data security policies are adhered to consistently across all data controller departments. Such measures would seek to ensure that the unauthorised removal of encryption software against the data controller's security policies is prevented, thereby removing any potential for unauthorised access to that personal data.

(2) Portable and mobile electronic devices, including laptops, which are 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. Where such encryption software is genuinely incompatible with a programme performing a necessary data controller function, then the data controller must ensure other adequate means of ensuring data is held securely are implemented. This might include the use of a secure network system for the storage of such personal data.

(3) Physical security measures are adequate to prevent unauthorised access to personal data. This includes adequate security management of areas that are not operational out of hours, adequate monitoring of swipe card door access and the effective use of security patrols.

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

Dated..... 5th July 2010

Signed....
Sarah-Jane Marsh
Chief Executive
For and on behalf of Birmingham Children's Hospital NHS Foundation Trust

Signed.....
Mick Gorrill
Head of Enforcement
For and on Behalf of the Information Commissioner