ICO Ref: ENF0372602

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: University Hospital of South Manchester NHS Foundation Trust

Wythenshawe Hospital
Southmoor Road
Wythenshawe
Manchester
M23 9LT

I, Julian Hartley, Chief Executive**,** of University Hospital of South Manchester NHS Foundation 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. University Hospital of South Manchester 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 by the data controller, informing that an unencrypted memory stick containing sensitive personal data had been lost by a medical student. The personal data on the memory stick related to approximately 87 patients and included patient name, age, occupation and details of the operation, specifically hand surgery.

3. The medical student was engaged in an audit within the Burns and Plastics Department at the University Hospital of South Manchester. It was assumed that the student had received data protection training at medical school, which was not the case, and therefore the student had not received an induction or training in this area.

4. The Trust provided the student with an encrypted memory

stick, containing the relevant data for the purposes of the audit. On completion of the placement, the student was asked to continue with the research by the data controller. As a result, the student copied the data from the Trust's encrypted memory stick on to a personal unencrypted memory stick. It was this personal device which was subsequently lost by the student.

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 health of the data subjects. Personal data containing such information is defined as "sensitive personal data" under section 2 of the Act. It was noted that this data was unlikely to be of the kind that would cause substantial damage or distress to the individuals concerned.

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. Students are provided with an appropriate induction to the data controller's policies and procedures in respect of data security at the beginning of any placement undertaken;

2. Staff and students are aware of the data controller's policy for the storage and use of personal data, specifically in respect of the use of personal or unencrypted portable devices, and are appropriately trained how to follow that policy;

3. Access to personal data for non-clinical purposes such as research and education is appropriately and regularly monitored for compliance with the data controller's policies on data protection and IT security;

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…….

Signed……

Julian Hartley
Chief Executive
University Hospital of South Manchester NHS Foundation Trust

Signed……

Sally Anne Poole
Head of Enforcement
For and on behalf of the Information Commissioner