ICO Ref: **ENF0377507**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: The Royal Liverpool and Broadgreen University Hospitals NHS Trust

The Royal Liverpool University Hospital
Prescot Street
Liverpool
L7 8XP

I, Tony Bell, Chief Executive, of the Royal Liverpool and Broadgreen University Hospitals NHS Trust, for and on behalf of the Royal Liverpool and Broadgreen University Hospitals NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The Royal Liverpool and Broadgreen University Hospitals NHS 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 Authority 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 notified of two separate incidents involving the loss of personal data.

3. One incident involved ward handover sheets containing details of 22 patients that were found in a street near to the hospital. The sheets contained names and details relating to medical conditions, but not addresses and had been taken off-site by mistake. Further enquiries revealed that if the correct procedures had been followed, this information would have been securely destroyed on site at the end of the working day.

4. A second incident involved the theft of a clinic bag from a car containing paper documents of 27 patients including

information relating to medical conditions ("sensitive personal data" as defined by the Act). Enquiries revealed that the breach arose because a member of Trust staff who was working from a community clinic was unable to remotely access the Trust's server to input the patient data. Instead they put the information into their clinic bag with the intention of inputting the information upon their return to the hospital.

5. Although each separate incident did not involve a large quantity of personal data, they occurred within a six month period suggesting that the data controller did not take sufficient measures to safeguard the personal data it held. The Commissioner has taken into account the fact that a proportion of the personal data in question related to medical conditions and could potentially result in distress being caused to the individuals concerned. It has been noted that the Trust has introduced remedial measures as a result of these incidents.

6. 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 disclosed in this incident consisted of information as to the physical or mental health or condition of the patient. 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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The data controller shall ensure that its policies in respect of the security of personal information, particularly the storage and use of "sensitive personal information" are adequate, clear and that staff are

adequately trained on how to fulfil their obligations under such policies;

(2) Compliance with the data controller's policies on data protection and IT security issues is appropriately and regularly monitored;

(3) A formal policy be written and implemented for appropriate staff for the handling and disposal of patient based information at the end of each working day that they are not required to retain using confidential waste depositories;

(4) In terms of community clinics remote access to the Royal Liverpool trust server, the data controller shall develop a robust process for reporting access issues and staff should receive appropriate additional training and support in line with that process;

(5) Technical problem with remote access to the Royal Liverpool Trust server is addressed;

(6) 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.

(7) The data controller shall agree to an audit by the ICO and the implementation of any recommendations.

Dated……..

Signed……

Tony Bell
Chief Executive
The Royal Liverpool and Broadgreen University Hospitals NHS Trust

Signed……

Sally Anne Poole

ICO Ref: **ENF0377507**

Acting Head of Enforcement
For and on behalf of the Information Commissioner