ICO Reference: ENF0390482

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: **Dartford and Gravesham NHS Trust**

Darent Valley Hospital
Darenth Wood Road
Dartford
Kent
DA2 8DA

I, Susan Acott, Chief Executive of Dartford and Gravesham NHS Trust, for and on behalf of Dartford and Gravesham NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Dartford and Gravesham 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 Dartford and Gravesham NHS 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 data controller informed the Information Commissioner (the "Commissioner") of a data security incident involving the potential loss of six boxes, estimated to contain in excess of 10,000 archived records.

3. The data controller advised the Commissioner that its records management policy required the records to be stored on the wards; however, at the time of the incident, dedicated storage areas were temporarily unavailable. As a stop-gap, boxes containing the records were kept in a ward waste-disposal room. The intention was to relocate the records once storage areas were accessible. Unfortunately, this did not happen and in the Trust's view it is likely that the boxes containing the records were removed and securely destroyed. In the absence of a clear and documented audit trial the Trust has been unable to ascertain the likely date of destruction. For the same reason, the Trust is also unable to specify how many

records contained personal and sensitive personal data.

4. The data controller has also explained that, although it considers that the storage of data within the waste-disposal room did not conform to its data handling policies, access to the room was restricted by key code. The data controller has confirmed that the loss of the records does not pose a clinical risk to the affected patients.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of these matters. 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 involved in the 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 of the Act.

6. Having considered the remedial action that has been taken by the data controller and the relevant policies in place at the time of the incident, 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) Staff are aware of the data controller's policies for the storage of personal data and are appropriately trained how to follow that policy;

(2) Compliance with the data controller's policies on data protection and storage of personal data is appropriately and regularly monitored;

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

(4) Destruction of personal and sensitive personal data should only be carried out in accordance with the data controller's policies and procedures.

Dated…….

Signed……

Susan Acott
Chief Executive, Dartford and Gravesham NHS Trust

Signed……

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