DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Sutton

Civic Offices
St Nicholas Way
Sutton
Surrey
SW1 1EA

I, Paul Martin, Chief Executive of London Borough of Sutton, for and on behalf of London Borough of Sutton hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. London Borough of Sutton 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 London Borough of Sutton 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 informed of several data security incidents by the data controller.

3. A paper file containing personal data relating to 73 individuals receiving social care went missing from an office.

   A document package relating to childcare proceedings was left with a neighbour of the intended recipient by a courier used by the data controller and subsequently went missing

   An unencrypted laptop was stolen from a locked cupboard on a children's hospital ward. The laptop contained personal data relating to 9 children being taught by a teacher employed by the data controller.

   An unencrypted laptop containing social care data relating to 39 individuals was stolen from the home of an employee of the data controller.

   9 administration computers used to access data on the data controller's network servers were stolen but some files may have been downloaded onto the computer hard drives in breach of policy.

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 these incidents 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 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) 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) Physical security measures are adequate to prevent unauthorised access to personal data;

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

(4) The policy covering the storage and use of personal data is followed by staff;

(5) 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..... 29th July 2009

Signed.....
Paul Martin, Chief Executive, London Borough of Sutton

Signed.....
Mick Gorrill
Assistant Commissioner, Regulatory Action Division
For and on behalf of the Information Commissioner