DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Shropshire Council

Shirehall
Abbey Foregate
Shrewsbury
Shropshire
SY2 6ND

I, Kim Ryley, Chief Executive of Shropshire Council (the Council), Shirehall, Abbey Foregate, Shrewsbury, Shropshire, SY2 6ND, for and on behalf of the Council hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Shropshire Council 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 Council 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 from the Council regarding a memory stick containing a social care management database. The memory stick was lost during postal transfer from Shropshire Council's offices to a regular contractor based in Cardiff.

3. Sensitive data was transferred onto a password protected but unencrypted memory stick in breach of Council procedure. The information related to 3554 social care clients and 188 members of staff. The memory stick was sent in inadequately protected packaging, and contained records that were excessive for their purpose and out of date. The Council's investigations into the incident revealed a number of other shortcomings regarding localised data storage and transmission procedures, which have also been taken into consideration.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Third and Seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data lost 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 Third and Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) Databases should only contain information relevant for their purpose and for the process of transfer;

(2) 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 by no later than 30 April 2010 using encryption software which meets the current standard or equivalent;

(3) Personal data should only be transferred to removable media when absolutely necessary. Where possible, sensitive personal data should be accessed remotely or hand-delivered. All other post should be adequately tracked and protected;

(4) Adequate checks are carried out on contractors' staff to ensure that data processors are complying with the data controller's policy in respect of the storage and transfer of such data ;

(5) The policy covering the transfer, storage and use of personal data is reviewed to ensure compliance with the Act, particularly in respect of the security of the means of transfer and relevance of the data transferred;

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

(7) 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.

Dated... December 3rd 2009.

Signed...
Kim Ryley
Chief Executive
Shropshire Council

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