

# DATA PROTECTION ACT 1998

## UNDERTAKING

Data Controller: Tees, Esk and Wear Valleys NHS Foundation Trust

West Park Hospital,  
Edward Pease Way,  
Darlington,  
County Durham,  
DL2 2TS.

I, Martin Barkley, Chief Executive of Tees, Esk and Wear Valleys NHS Foundation Trust, West Park Hospital, Edward Pease Way, Darlington DL2 2TS for and on behalf of Tees, Esk and Wear NHS Foundation Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Tees, Esk and Wear Valleys 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 Tees, Esk and Wear Valleys NHS Foundation 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 Commissioner was informed by the Trust's self reported breach of data security that an unencrypted data stick holding personal data and sensitive personal data relating to health patients and also to Trust staff was lost. The data stick was then found by a member of the public who passed it to the press. The Commissioner notes that the Trust initiated an investigation and that a report into the incident will subsequently be made available.
3. The Commissioner has considered the Trust's remedial action taken to date, the intended further remedial action and the Trust's compliance with the provisions of the Act in 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 1 of the Act.
4. Following consideration of the various remedial action and the fact that the data controller recognises the seriousness of the matter, 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 or from other data controllers in similar circumstances, ensure that personal data is processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part 1 of the Act, and in particular that:

- only data sticks with an appropriate standard of encryption are used by Trust staff and external contractors working for the Trust and that sufficient guidance on their use is given;
- an adequate encryption policy and procedures on encryption are put in place and steps taken to ensure that Trust staff and external contractors are made fully aware of the policy and procedures and adhere to them;
- sufficient checks are put in place to ensure, where appropriate, that external contractors are made fully aware of the Trust's information governance and data security issues with regard to the work they undertake;
- the Trust protocol, currently being developed, on the use of all forms of mobile storage devices is sufficiently rigorous to prevent an incident of this nature from occurring again; and
- on an ongoing basis, adequate and relevant data protection training is provided to appropriate Trust employees and shall include training on the Seventh Data Protection Principle.

Dated..... 2/11/09 .....

Signed.....  
For and on behalf of Tees, Esk and Wear Valley NHS Foundation Trust

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