

# DATA PROTECTION ACT 1998

## UNDERTAKING

Data Controller:                   NHS Lothian

  Deaconess House  
  148 Pleasance  
  Edinburgh  
  EH8 9RS

I, James Barbour, Chief Executive of NHS Lothian, Deaconess House, 148 Pleasance, Edinburgh EH8 9RS, for and on behalf of the NHS Lothian hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. NHS Lothian 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 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 Information Commissioner (the "Commissioner") was provided with two reports from the data controller, regarding the temporary loss of a document wallet, left in a shop, containing 25 paper files containing personal data of home based patients and the loss of a USB memory stick containing personal data of 137 patients. The memory stick was the personal property of an employee and therefore should not have been used to store NHS Lothian personal data. The memory stick was also not encrypted to ensure an adequate level of data security. These events occurred in June 2008 and in both cases the employees involved failed to comply with NHS Lothian security requirements
3. 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 1 of the Act.
4. Following consideration of the remedial actions that have 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 or from other data controllers in similar circumstances, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part 1 of the Act, and in particular that:**

- (1) Portable and mobile devices including memory sticks 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) Network systems are introduced to prevent the use of unauthorised or personal memory devices or computer systems to download personal data being processed by NHS Lothian;**
  
- (3) The data controller shall take all reasonable measures to ensure the physical security of any paper files containing personal data, whether those files are on the data controller’s own premises or in transit to other locations including patients’ homes;**
  
- (4) The data controller shall ensure that all staff are adequately trained on the data controller’s information security policies;**
  
- (5) The data controller shall implement such other security measures it deems appropriate to ensure that personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage.**

Dated.....

Signed.....

James Barbour  
Chief Executive  
NHS Lothian

Signed.....

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