

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Hastings and Rother Primary Care Trust

Bexhill Hospital
Holliers Hill
Bexhill-on-Sea
East Sussex
TN40 2DZ

I, [NAME REMOVED], [JOB TITLE REMOVED] of Hastings and Rother Primary Care Trust (the Trust), Bexhill Hospital, Holliers Hill, Bexhill-on-Sea, East Sussex, TN40 2DZ, for and on behalf of the Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Hastings and Rother Primary Care 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 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 a report from [NAME REMOVED] acting on behalf of the data controller, regarding the theft of a desktop computer which contained the personal data of patients of the data controller, including some data relating to the health of those patients ("sensitive personal data" as defined by the Act). It is believed that the computer was stolen by an opportunistic thief who had entered the building via scaffolding that was not normally in place. The data controller did not own the building in which this incident occurred, but had raised concerns over the building's security. However, the data controller did not take its own measures to safeguard the personal data it held at these premises.
[INFORMATION REMOVED]
3. 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 1 of the Act.
4. 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 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) The data controller shall take all reasonable measures to ensure the physical security of any of its own equipment that is used to process personal data, whether that equipment is on the data controller's own premises or on the premises of another organisation;**
- (2) The data controller shall ensure that its policies on the storage of personal data are clear and that staff are adequately trained on how to fulfil their obligations under such policies;**
- (3) 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.....

[NAME REMOVED]

[JOB TITLE REMOVED]

Hastings and Rother Primary Care Trust

Signed.....

Mick Gorrill

Assistant Commissioner Regulatory Action Division

For and on behalf of the Information Commissioner