

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Maidstone and Tunbridge Wells NHS Trust
Hermitage Lane,
Maidstone,
ME16 9QQ

I, Mr Glenn Douglas, Chief Executive of Maidstone and Tunbridge Wells NHS Trust, Hermitage Lane, Maidstone, ME16 9QQ, on behalf of Maidstone and Tunbridge Wells NHS Trust, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Maidstone and Tunbridge Wells NHS 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 on by Maidstone and Tunbridge Wells NHS 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 the Director of ICT regarding the theft of an unencrypted laptop computer from the Audiology Department in July 2009. The laptop computer contained the personal data and sensitive personal data of 33 patients between 2006 and 2009 and an unknown number of patients between 2003 and 2006. Three encrypted laptop computers belonging to the data controller were also stolen in August 2009 from the Maidstone site.
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 at Part I of Schedule 1 to the Act.
4. In view of the circumstances of this incident and the remedial steps taken by the data controller as a result, it has been 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 is processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act,

and in particular that:

- **The data controller shall ensure, within six months, that any personal data held on a laptop computer or other removable media by the data controller is identified and encrypted so as to provide effective protection against unauthorised access;**
- **The data controller shall implement such security measures as it deems appropriate to ensure that personal data is more effectively protected from theft and implement any other measures to ensure against unauthorised or unlawful processing, accidental loss, destruction and/or damage.**

Dated.. 16 10 09

Signed. [Redacted]
For Maidstone and Tunbridge Wells NHS Trust

Signed.. [Redacted]
Mick Gorrill (Assistant Commissioner, Regulatory Action Division)
For the Information Commissioner