

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Mid Staffordshire NHS Foundation Trust.

Weston Road
Stafford
ST16 3SA

I, Antony Sumara, Chief Executive, of the Mid Staffordshire NHS Foundation Trust for and on behalf of the Mid Staffordshire NHS Foundation Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The Mid Staffordshire 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 Mid Staffordshire 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. On 16 June 2009, the Information Commissioner (the "Commissioner") received a complaint in respect of a data security breach concerning Mid Staffordshire NHS Foundation Trust data.
3. This matter arose as a result of a member of the trust's HR department transferring to, and saving, a 'Statement of Case', which contained sensitive personal information in relation to a Trust employee and two further Trust documents, on a home computer in contravention of Trust policy. The information in question was not password or encryption protected.
4. Having been informed of this security breach, the Trust initially failed to demonstrate appropriate urgency in the securing of the data concerned.
5. 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 I to the Act.

6. The Commissioner has also considered the fact that some of the data concerned in this incident consisted of information relating to a criminal conviction in respect of the data subject. Personal data containing such information is defined as "sensitive personal data" under section 2 of the Act.
7. 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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. **Physical security measures are adequate to prevent unauthorised access to, and or transfer of, personal data;**
2. **The policy covering the storage and use of personal data is followed by staff, particularly in respect of staff working from home;**
3. **Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy. Consideration should be given to the provision of periodic refresher training and the 'dip sampling' of staff understanding of the policy;**
4. **The data controller shall implement a formal 'Working from home' policy which will ensure the security of Trust data accessed from any such remote site. The policy to be introduced within 3 months from the date of the signing of this undertaking;**
5. **Trust policies are amended as appropriate to include explicit reference to staff data in terms of protecting personal information;**
6. **The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

7. **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 using encryption software which meets the current standard or equivalent;**
8. **Where a data security breach is suspected, the data controller will take appropriate remedial action as soon as practicable to ensure the recovery of, or prevent access to, any data rendered insecure;**
9. **The Trust IT Security policy to be amended to require that where a data security breach is suspected the Director of Nursing and Governance is informed as soon as practicable.**

Dated..... 2 / 10 / 09

Signed.....

Antony Sumara
Chief Executive
Mid Staffordshire NHS Foundation Trust.

Signed.....

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