Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

UNDERTAKING

Data Controller: **The Department of Health**

Head Office:

Room 352C
Skipton House
80 London Road
London
SE1 6LH

The Department of Health, Room 352C, Skipton House, 80 London Road, London SE1 6LH hereby acknowledges the details set out as follows:

1. The Department of Health 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 the Department of Health 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 (ICO) has received a complaint regarding the processing of personal data by the data controller, and in particular that the personal details of junior doctors held on the Medical Training Application Service (MTAS) website was readily accessible to any person accessing the website.

3. The ICO 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 1 of Schedule 1 to the Act. A copy of the Data Protection Principles is attached.

4. By letters dated 24 May 2007, 21 June 2007, and 21 September 2007 the data controller made representations to the ICO.

Information Commissioner's Office

Following consideration of those representations it has been agreed that, in consideration of the ICO not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes to comply with the terms of the following undertaking:-

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 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,

- ***Personal data which if disclosed could cause damage or distress, for which the Department of Health is the data controller and which is held on any website, either by the data controller or a data processor carrying out work on behalf of the data controller, is suitably encrypted so as to provide effective protection against unauthorised access.***
- ***Instructions and advice as to the use of passwords and PIN numbers be given by the data controller to those entitled to access the site.***
- ***Adequate and relevant Data Protection training will be given to appropriate staff on an ongoing basis***
- ***Adequate and effective contract management will be in place to confirm that technical and organisational security measures governing any processing by those acting on the data controller's behalf are being complied with.***
- ***There is regular 'penetration and vulnerability' testing of developing applications and systems to minimise unauthorised access.***
- ***regular monitoring of the MMC Application website (the replacement for MTAS) which was undertaken during the recent round of applications for posts will be carried out during future rounds. The objective is to ensure that the systems in place to provide effective protection against unauthorised access are operating correctly.***
- ***The data controller shall implement such other security measures it deems appropriate to ensure personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage.***

Dated..... 4/12/07

Signed...
For The Department of Health

Signed.
Mick Go Action Division)
For the Information Commissioner