

## DATA PROTECTION ACT 1998

### UNDERTAKING

Data Controller: **Independent Parliamentary Standards Authority**

**7<sup>th</sup> Floor, Portland House  
Bressenden Place  
London  
SW1E 5BH**

I, Andrew McDonald, interim Chief Executive Officer of the Independent Parliamentary Standards Authority, for and on behalf of the Independent Parliamentary Standards Authority hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

The Independent Parliamentary Standards Authority 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 Independent Parliamentary Standards Authority 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.

The Information Commissioner (the "Commissioner") was informed that a database recording MPs expenses had been rendered temporarily insecure following IT maintenance.

On 13 July 2010, for a period of some 21 hours, information relating to the expenses claims of various Members of Parliament was inadvertently made available to all those MPs, and their nominated staff, with access to the internal "Expenses@work" (E@W) IT system. The data compromised was of some sensitivity and included MPs home telephone numbers, bank account details and vehicle registration details.

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.

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. Changes made to the E@W administrator accounts should be reviewed regularly.
2. Appropriate changes to the system are introduced so as to ensure that the 'reports' field cannot be left blank.
3. Breach notification procedures will be reviewed and communicated to all MPs and staff.
4. The data controller shall implement such other security measures as, and when, it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Dated.....

Signed.....

Andrew McDonald  
Interim Chief Executive.  
Independent Parliamentary Standards Authority.

Signed.....

Mick Gorrill  
Head of Enforcement  
For and on behalf of the Information Commissioner

