

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Cardiff and Vale University Health Board

Executive Medical Director
Whitchurch Hospital
Cardiff
CF14 4XW

I, Dr Graham Shortland, Executive Medical Director (Caldicott Guardian) Cardiff and Vale University Health Board, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Cardiff and Vale University Health Board 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 Cardiff and Vale University Health Board 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 informed on 26 November 2012, of the loss of a consultant psychiatrist's bag. The bag contained sensitive personal data including, a mental health act tribunal report relating to a patient, a solicitor's letter, five CV's for consultant job applications and personal valuables, including a purse and a mobile phone. The bag was lost whilst the consultant was cycling home from the data controller's business premises.
3. The documents were contained in a rucksack that the consultant had believed to be securely fastened to a child seat. The data was required in order for the consultant to undertake work outside of the office environment.
4. Further investigation by the Commissioner's staff determined that the consultant attended induction training in November 2012. This had taken place post incident and did include data protection training. The data controller was therefore unable to demonstrate that mandatory data protection training was fully implemented.
5. The data controller has confirmed that alternative means of transporting the data, such as the use of an encrypted portable device, or remote server access were available. However, these options were not communicated clearly to staff and procedures to document the processes that need to be followed were lacking.

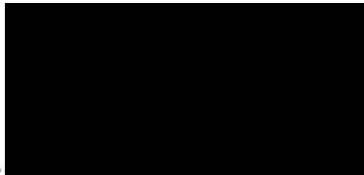
6. Further, the data controller has confirmed that no relevant protective marking schemes were in place at the time of the incident. In the Commissioner's view this suggests a lack of data protection awareness with regards to implementing adequate controls around the removal of information for use off-site.
7. The Commissioner has considered the data controller's compliance with the provisions of the Act in 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. The Commissioner has also considered the fact that some of the data involved consisted of information relating to the health of the data subjects. Such information is considered 'sensitive personal data' as defined in section 2(e) of the Act.
8. 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) The data controller shall put in place an adequate security policy for the removal of documentation off site and the security of the data whilst in transit. All staff shall be made aware of that policy and trained in how to follow it;**
- (2) All data protection training be made mandatory in relation to both the requirements of the Act and the data controller's policies relating to the use of personal data. Completion of such training shall be recorded and monitored to ensure compliance;**
- (3) Where appropriate, any staff are assessed for their suitability for home working and appropriate arrangements made for the most secure method of transporting the relevant data;**
- (4) The data controller shall put into place an appropriate protective marking scheme and make use of redaction techniques where possible;**
- (5) Compliance with the data controller's policies on data protection and IT security issues shall be appropriately and regularly monitored;**

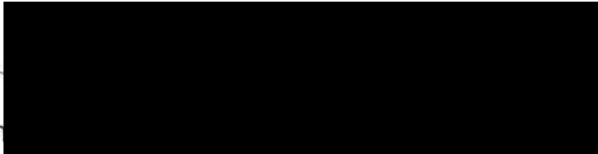
(6) The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Dated on publication



Signed ..

.....
Dr Graham Shortland, Executive Medical Director (Caldicott Guardian)
Cardiff and Vale University Health Board



Sign
Stephen Eckersley, Head of Enforcement
For and on behalf of the Information Commissioner

