

## **DATA PROTECTION ACT 1998**

### **UNDERTAKING**

Data Controller: Wokingham Borough Council

Civic Offices  
Shute End  
Wokingham  
RG40 1BN

I, Andy Couldrick, Chief Executive of Wokingham Borough Council (the 'Council') for and on behalf of the Council, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Wokingham Borough Council 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 Council 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 that documents requested by a service user by means of a subject access request (SAR) under the Act had been hand-delivered to her address but that the package had been left on the doorstep as no-one was home. The DC's policy did make clear that SARs should be delivered by secure means but the delivery driver had no instructions to obtain a signature or return the package to the data controller's offices. When the delivery driver (who was employed by the data controller) went back past the property some 2.5 hours later, the package had disappeared and it was assumed the requester had taken it inside.
3. The documents contained sensitive personal data relating to the requester and her children, who had been subject to social services intervention due to allegations of neglect and abuse by the requester's ex-partner. They included a report prepared for the courts in relation to these issues and the children's welfare.
4. The Commissioner's investigation revealed that the incident resulted from a series of errors and failures in communication among the data controller's employees in various departments. Despite the sensitivity of the documents, the courier was not provided with clear instructions not to leave the documents without obtaining the requester's signature. The requester had not confirmed to the data controller's social services team that she would be able to accept delivery on the date proposed, yet delivery

was still arranged.

5. However, it was also established that the data controller's employees are provided with training relating to data protection and information security only when they join the organisation. After that, the data controller promotes this training to existing staff but take-up is not compulsory, although training in other areas is provided on a mandatory basis for all staff.
6. The Commissioner was aware of previous cases in respect of which his office had not taken formal regulatory action, but had provided advice to the data controller. Part of this advice had been on the subject of training and employee awareness of data protection, and the Commissioner had strongly recommended mandatory training which would be regularly refreshed for all employees whose roles involved access to personal data. The investigation into this incident revealed that these recommendations had not been properly implemented by the data controller.
7. 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. The Commissioner has also considered the fact that some of the data involved in this incident consisted of information as to the physical or mental health or condition of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under 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) All staff shall be made aware of the data controller's policy and procedures for the storage and use of personal data, and appropriately trained how to follow these, by 31 July 2014;**
- (2) Training in data protection and information security, including the data controller's policy and procedures in these**

**areas, shall be carried out prior to initially granting access to the data controller's systems for all staff whose roles involve regular access to personal data; a refresher training structure shall be implemented so that training shall be regularly updated and refreshed at regular intervals, not exceeding two years, by 31 July 2014;**

- (3) Procedures shall be drafted and implemented to cover such issues as transporting paper records containing personal data outside the office environment, by no later than 30 June 2014;**
  
- (4) Compliance with the data controller's policies on data protection and completion of the above-mentioned training shall be appropriately and regularly monitored, and appropriate steps taken to ensure any failings are rectified with minimal delay;**
  
- (5) 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.**

Signed .....  
Andy Couldrick  
Chief Executive  
Wokingham Borough Council

Dated: .....

Signed .....  
Steve Eckersley  
Head of Enforcement  
For and on behalf of the Information Commissioner

Dated: .....