

## **DATA PROTECTION ACT 1998**

### **UNDERTAKING**

Data Controller: Leeds City Council

Civic Hall  
Leeds  
LS1 1UR

I, Tom Riordan, Chief Executive, of Leeds City Council, for and on behalf of Leeds City Council, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Leeds City 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 Leeds City 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 by the data controller that a private area on the Leeds Initiative website was accessible to members of the public. The personal data that was compromised was located in 7 excel spreadsheets and included name, address, date of birth and disability details.
3. The insecurity on the website only occurred when migration to a new server took place. The data controller used a data processor to undertake the migration. There was a failure by the data processor to configure the new server identically to the old server. On completion, the site was not sufficiently tested, so it was not identified that the private area was accessible. Contractual obligations were in place but it was not established whether the work was conducted under the data controller's or data processor's term and conditions.
4. 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 compromised 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.

5. 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, within three months of 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 ensure that clear and appropriate contractual arrangements are in place with any data processor employed;**
- (2) The data controller shall ensure that contracted data processors are appropriately monitored to ensure their compliance with the seventh principle;**
- (3) The data controller should ensure that, where necessary, technically proficient staff are included at all stages of the procurement process;**
- (4) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

Signed: .....

Tom Riordan  
Chief Executive  
Leeds City Council

Dated: .....

Signed: .....

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

Dated: .....