ICO Ref: **ENF0478131 and ENF0482620**

# DATA PROTECTION ACT 1998

# UNDERTAKING

Data Controller: Luton Borough Council

Town Hall
George Street
Luton
Bedfordshire
LU1 2BQ

I, Trevor Holden, Chief Executive of Luton Borough Council (the 'Council'), for and on behalf of the Council, hereby acknowledge the details set out below and undertake that the Council will comply with the terms of the following Undertaking:

1. Luton 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 reports of two separate incidents in which sensitive personal data was incorrectly handled by social work staff employed by the data controller. These incidents took place in December 2012 and January 2013.

3. In one incident, an email containing personal data about one family, together with advice to one individual, was sent unprotected across an internet connection and also misdirected to an agency dealing with a different family. In the other case, a social worker was advised to leave the office and return home due to severe weather and took with them the paperwork they'd worked on that day. Some of it, containing personal data about a vulnerable young person, was lost as the result of an accident on the journey home.

4. The Commissioner was aware of several previous incidents in respect of which his office had not taken formal regulatory action, but had given advice to the data controller. Part of this advice had been on the subject of training and employee awareness, and the Commissioner had strongly recommended mandatory training which would be regularly refreshed for all employees whose role involves access to personal data. The investigation into these incidents revealed that these recommendations had not been

properly implemented by the data controller.

5. 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, which is set out in Schedule 1, Part I to the Act.

6. The Commissioner has also considered the fact that some of the data in these incidents consisted of information as to the health or condition and the ethnicity of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2 of the Act.

7. Following consideration of the action that has already 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 no later than 30 November 2013;**

**(2) Training in data protection and information security, including the data controller's policies 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; and shall thereafter be refreshed and updated at regular intervals, not exceeding two years, with effect from 30 November 2013;**

**(3) Procedures shall be drafted and implemented to cover such issues as transporting personal data outside the office environment (to cover electronic and paper records), by no later than 30 November 2013;**

**(4) Compliance with the data controller's policies on data protection and IT security issues, and the completion of training by staff, shall be appropriately and regularly monitored;**

**(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.**

Dated on publication

Signed ……
Trevor Holden
Chief Executive
Luton Borough Council

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