

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Luton Borough Council

Apex House
30-34 Upper George Street
Luton
Bedfordshire
LU1 2RD

I, Trevor Holden, Chief Executive of Luton Borough Council, for and on behalf of Luton Borough Council, hereby acknowledge the details set out below and undertake to 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 Luton Borough 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 informed by the data controller on 21 January 2011 that a flaw had been discovered in a number of Council issued encrypted memory sticks. The flaw could permit the memory sticks to be formatted, removing the encryption protection. The data controller discovered the flaw when conducting a recall of old devices. During the recall process a total of 619 memory sticks were identified as having incomplete audit records, with the location of half of these being unknown.
3. It has been established that only a small percentage of the untraced devices will be subject to the encryption flaw. It is also likely that the majority of these contain no personal data. However, due to the circumstances, the actual risk to individuals is unknown.
4. Appropriate remedial action has been taken by the data controller and the appropriate auditing and security of such devices re-established.
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. This Principle is set out in Schedule 1, Part I to the Act.

6. 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) Portable and mobile devices including memory sticks and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software which meets the current standard or equivalent. Such measures must ensure that unauthorised removal of encryption software is prevented.**
- (2) Staff are made aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;**
- (3) The data controller's policy in respect of access to end points used to transfer personal data to portable media will be reviewed and appropriate controls agreed and implemented by 1 January 2012;**
- (4) A detailed audit trail will be maintained in respect of all portable media devices used to store personal data;**
- (5) A home working policy will be introduced, or the current agile working policy amended, to stipulate the precise circumstances in which any portable media device or any other personal data can be removed from the normal business premises. This will include details of the degree of security to be applied to such media or data when away from the premises;**
- (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.....

Signed.....

Trevor Holden

ICO Ref: **ENF0370351**



Chief Executive
Luton Borough Council

Signed.....

Sally Anne Poole
Head of Enforcement
For and on behalf of the Information Commissioner