ICO Ref: **ENF0401638**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Bolton Council
Town Hall
Bolton
BL1 1RU

I, Sean Harriss, Chief Executive of Bolton 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. Bolton 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. In July 2011, the Information Commissioner (the "Commissioner") received a report from the data controller about the theft of a rucksack from a keyworker's car. The bag contained hard copy documentation that featured various types of sensitive personal data relating to several individuals. A second incident was also reported at the same time involving an email sent in error to several hundred people, all of whom either worked for, or with, the data controller. Attached to the email was a completed occupational health form for one employee.

3. Enquiries into the first incident indicated that most keyworkers' duties are carried out offsite in a responsive manner, so some reference documents are required. However, despite having access to secure storage facilities, the employee in question was carrying significantly more paperwork than necessary to perform their duties, without the knowledge of management. Further investigations revealed that despite the fact many employees are predominantly mobile workers, the data controller had not sufficiently explored the implications of handling personal data in a mobile environment, and risk assessments were lacking. However, the data controller did have policies in place covering removal of personal data from the office, and the employee had previously received appropriate training.

4. In the second case, it transpired that autofill is often used when sending emails, and that existing email groups do not differentiate between internal and external addresses.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of these matters. 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 these incidents consisted of information as to the ethnic origin of the data subjects and/ or their physical or mental health or condition. Personal data containing such information is defined as "sensitive personal data" under sections 2(a) and (e) of 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. Hard copy documentation is only removed from the office or secure storage when absolutely necessary. It will contain the minimum amount of personal data required for its purpose and will be anonymised where possible;

2. Thorough risk assessments are completed for all mobile working arrangements;

3. Staff are aware of the data controller's policies on the retention, storage and use of personal data, and are appropriately trained how to follow those policies;

4. Compliance with the data controller's policies on data protection and IT security is 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…….

Signed……
Sean Harriss
Chief Executive
Bolton Council

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