ICO References ENF0371208 & ENF0402668

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Brighton & Hove City Council

Hove Town Hall, Norton Road, Hove,
BN3 3BQ

I, John Barradell, Chief Executive, of Brighton & Hove City Council, for and on behalf of Brighton & Hove City Council hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Brighton & Hove 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 Brighton & Hove 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 informed by a third party about data security issues relating to the processing of personal data by Council sessional workers. These workers are recruited in the same way as permanent staff but are casual employees under contract for specific assignments. Sessional workers are used mainly to supervise contact between children in care and family members. The necessary anonymised information is sent to the sessional worker by email prior to the contact.

   A written report of the contact has to be submitted to the Council within 48 hours. These reports are often required by Courts and can be used in evidence.

3. In May 2009 a sessional worker had his unencrypted personal laptop stolen during a burglary. The Council has explained that the laptop was thought to have contained some sensitive personal data relating to up to seven families. At the time of the incident sessional workers did not have access to the Council's secure computer network, the secure email system or to encrypted laptop computers and the information was not anonymised. The Council did not report the incident to the ICO at the time due to the low volume of personal data involved. The Commissioner recognises that the Council has already put measures in place to reduce the likelihood of a similar incident including the anonymisation of information and that it has taken steps to allow sessional workers the necessary access to the Council's secure systems. The Commissioner does however consider it necessary for the data controller to take further steps, as set out in this undertaking.

4. In addition the Council informed the ICO that on 1 July 2011 a copy of an employee's data had been sent by email to 2821 Council employees in error. The data in question included details of income and salary deductions. The email address used in error is only needed by ICT employees and it has now been hidden from other employees. A prompt recall and the time the email was sent (16:30 on a Friday) meant that the disclosure was limited. The emails were later deleted from the system.

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 involved is likely to have consisted of information defined as "sensitive personal data" under section 2 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. Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, will within two months of the date of this Undertaking be encrypted using appropriate encryption software which meets the current standard or equivalent;

2. There is a suitable secure means of transferring personal data between the Council and their sessional workers in place and that the appropriateness of this is reviewed at regular intervals;

3. Physical security measures are adequate to prevent unauthorised access to personal data;

4. Appropriate administrative measures are in place to control employee use of email groups;

5. All staff are aware of the Council's policy for the retention, storage and use of personal data and are appropriately trained how to follow that policy;

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……
John Barradell
Chief Executive
Brighton & Hove City Council.

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