

# DATA PROTECTION ACT 1998

5/3/10

## UNDERTAKING

Data Controller: St Albans City and District Council

Civic Centre  
St Peters Street  
St Albans  
Hertfordshire  
AL1 3JE

I, Daniel Goodwin, Chief Executive Officer, of St Albans City and District Council for and on behalf of St Albans City and District Council hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. St Albans City and District 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 St Albans City and District 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 St Albans City and District Council's Head of Internal Audit section, in a letter dated 10 November 2009, that the Council had suffered a theft of four laptop computers. The matter was also reported by a number of residents affected by the incident.
3. On a date prior to 23 June 2009 a large number of postal voters records were stored on a password protected, but unencrypted, laptop computer. The storage of the data by this means met Council IT security policy at that time.
4. On conclusion of the election process the, now redundant, data was not removed from the laptop computer within a reasonable period of time.
5. The laptop computer in question was locked away in a safe in the elections department. However on the 15 June 2009, in response to a support call the laptop was taken by contracted IT staff (working for Northgate Information Solutions Ltd). The laptop was taken to the council's IT section, part of which is occupied by NIS staff.

6. It appears that the laptop in question was then not made subject of appropriate security, not being locked away or subject of a Kensington type lock. It appears that the laptop may have been left in open view on a desk within the Council's IT section for a period of some weeks. The laptop was recorded as having been present in the IT section on 23 June 2009.
7. On 22 September 2009 the Council's Head of IT Services discovered the laptop and requested a member of staff to secure it. It appears that the laptop was moved to another desk within the department, but not secured.
8. On 13 October 2009 three other laptop computers, which did not contain any personal information, were discovered to be missing. On 5 November 2009 the laptop computer containing personal data was discovered to be missing. All four laptop computers were believed to have been stolen.

The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Fifth and Seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act.


Following consideration of the comprehensive 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:

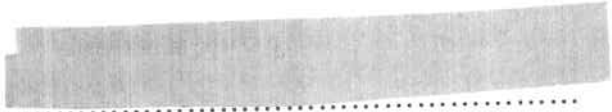
**The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Fifth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, 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, are encrypted using encryption software which meets the current standard or equivalent;**
- (2) Physical security measures are adequate to prevent unauthorised access to personal data;**
- (3) Adequate security checks are carried out on contractors' staff, and that such staff are made aware of the Council's IT security policy;**

- (4) The policy covering the storage and use of personal data is followed by staff;
- (5) Staff are aware of the data controller's policy for the storage and use of personal data, particularly in respect of keeping data only for as long as its purpose requires, 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..... *St March 2010* .....

Signed.   
Mr Daniel Goodwin  
Chief Executive Officer  
St Albans City and District Council

Signed.   
Mick Gorrill  
Assistant Commissioner, Regulatory Action Division  
For and on behalf of the Information Commissioner