

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Alzheimer's Society

Devon House
58 St Katharine's Way
London
E1W 1JX

I, Ruth Sutherland, Chief Operating Officer of the Alzheimer's Society (the Society), for and on behalf of the Society, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The Alzheimer's Society 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 Society 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 a report that several unencrypted laptop computers, one of which contained personal data relating to around 1,000 staff, were stolen from the data controller's Cardiff office during a burglary at the end of August 2009.
3. The laptops had been returned to the office for encryption, but this had not yet taken place when the theft occurred. One machine contained names, addresses, National Insurance numbers and salary details for staff across England, Wales and Northern Ireland, held in an Excel spreadsheet. The laptops were neither physically secured by cable locks, nor locked away securely. This was the third data security incident reported by the data controller to the Commissioner during 2009. The Commissioner's enquiries also revealed that staff did not receive any formal data protection training.
4. 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.
5. 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, 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) Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;
- (4) 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..... 1 February 2010

Signed....
Ruth Sutherland
Chief Operating Officer
Alzheimer's Society

Signed.....
Mick Gorrill
Head of Enforcement
For and on behalf of the Information Commissioner