ICO Ref: ENF0460222

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Northern Health & Social Care Trust

The Cottage
5 Greenmount Avenue
Ballymena
County Antrim
BT43 6DA

I, Paul Cummings, Senior Director of Corporate Management, of Northern Health & Social Care Trust, for and on behalf of Northern Health & Social Care Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Northern Health & Social Care Trust 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 Northern Health & Social Care Trust 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 made aware of a number of security incidents which led to a formal investigation into the Trust's compliance with the Act. One incident in May 2011, involved confidential service user information being faxed from a ward in Antrim Hospital to a local business in error. The information was intended for the Trust's Community Rehabilitation Team. The referral form contained sensitive clinical data. However the information was returned promptly by the recipient and there was a fax policy in place that was not followed correctly. A further incident involved the inappropriate disclosure of minutes containing sensitive personal data to professionals working in partnership with the Trust.

3. The Commissioner's investigation into the Trust revealed that despite the Trust having introduced what should have been mandatory Information Governance training for all staff, the majority of staff involved in these incidents had not received

this training. This highlighted a potentially serious failing in respect of staff awareness of Information Governance policies. In particular, the failure to monitor and enforce staff completion of training was a concern.

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. The Commissioner has also considered the fact that some of the data compromised in these incidents consisted of information as to the physical or mental health or condition of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of 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. **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;**

2. **Sufficient measures are put in place to ensure that all staff attend mandatory training;**

3. **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;**

4. **Procedures are put in place to ensure any reported breach of security is acted upon promptly and any remedial measures enforced. Where necessary staff**

should receive appropriate additional training and support in this respect;

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

6. **The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

Signed: ……

Paul Cummings
Senior Director of Corporate Management
Northern Health & Social Care Trust

Dated: …….

Signed: ……

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

Dated: …….