ICO Ref: **COM0587506**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Northern Health and Social Care Trust

Trust Headquarters Bretten Hall
Antrim Area Hospital
Bush Road
Antrim
BT41 2RL

I, Dr Tony Stevens, Chief Executive, of Northern Health and Social Care Trust, for and on behalf of Northern Health and Social Care Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Northern Health and 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 and 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 notified by the data controller that 11 emails intended for a doctor's personal non-trust email account were sent to a member of the public with the same name over a two year period. Notification of these incidents led the Commissioner to undertake a formal investigation into the data controller's compliance with the Act.

3. The Commissioner's enquiries revealed that not all of the emails contained personal data. However a number of emails contained personal data that related to the intended recipient and on one occasion an email contained sensitive personal data relating to a patient. During the course of the investigation it was also discovered that none of the emails were securely protected in line with the data controllers email policy. Furthermore and although the recipient had advised the senders of the email's that they had been incorrectly sent to the wrong address, this was not escalated as an information governance incident. The data controller therefore

only became aware of the issue when the recipient's wife contacted the IG team directly.

4. The Commissioner considers that this incident along with previous incidents he has investigated and an audit he has conducted have uncovered some significant shortcomings in relation to staff training and staff awareness of policies and procedures. The Commissioner therefore considers that further steps to address these issues are required.

5. The Commissioner is particularly concerned that the take up of training is low. As of December 2015 the take up of Information Governance Awareness training was 60% and training delivered to managers on Processing of Personal Information (POPI) was 81%. The Commissioner is also concerned that staff were unaware of the policy and procedure for reporting IG incidents.

6. 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 this incident consisted of information as to the physical or mental health or condition of the data subject. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

7. 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. **The data controller must ensure that all staff, including locum doctors, 3rd Party contractors, temporary (agency/bank staff) and volunteers, whose role involves the routine processing of personal and sensitive personal data undertake mandatory data**

protection and data handling induction training and regular refresher training on the requirements of the Act.

2. **Provision of such training shall be recorded and monitored with oversight provided at a senior level against agreed Key Performance Indicators to ensure completion. In addition, the data controller shall implement follow-up procedures to ensure that staff who have not attended/completed training do so as soon as is practicable.**

3. **The data controller shall ensure that staff, including Locum doctors, 3rd party contractors, temporary (agency/bank staff) and volunteers are aware of the content and location of its policies and procedures relating to the processing of personal data, specifically the procedure for reporting and recording IG breaches. If not already in place, a mechanism to ensure that staff are updated of any changes to these policies and procedures should also be implemented.**

4. **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: .....

Dr Tony Stevens
Chief Executive
Northern Health and Social Care Trust

Dated: .....

Signed: .....

Ken Macdonald
Assistant Commissioner (Scotland & Northern Ireland)
For and on behalf of the Information Commissioner

Dated: .....