ICO Ref: ENF0517849

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Western Health & Social Care Trust

Admin Building
Altnagelvin Area Hospital
Glenshane Road
Londonderry
BT47 6SB

I, Elaine Way, Chief Executive, of Western Health & Social Care Trust , for and on behalf of Western Health & Social Care Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Western 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 Western 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 notified of two separate incidents involving the loss of personal data which led to a formal investigation into the Trust's compliance with the Act. One incident concerned the theft of two Trust Personal Computers as the result of a break-in to Trust premises on 8 October 2013. One computer contained sensitive personal data relating to the provision of specialist mental health services. The data related to the caseload of a retired member of staff. The information had been deleted from the desktop. However the Commissioner's investigations identified there was a risk that the data could still be retrieved from the hard disk.

3. Enquiries revealed that whilst this appeared to be an opportunist theft, additional technical measures could have prevented the possibility of the information being accessed. For example, sensitive personal data could have been stored offline in an encrypted system rather than a desk top hard drive. Further, the personal data could have been securely

deleted to a greater level of permanence from the hard drive by using a specific secure deletion tool.

4. It has been noted that the Trust had a Data Protection & Confidentiality Policy and ICT Security policy in place at the time of the incident. These explained how data of this type should be handled and staff's responsibilities in this regard. However, the Commissioner considers that further steps to ensure appropriate information management structures across the network is appropriate.

5. A further incident was reported to the Commissioner in June 2014 after photocopied medical records disclosed to an individual in response to a subject access request (SAR) contained information about two other patients. Enquiries revealed the patient notes for two unrelated individuals were misfiled in to the requester's records. Whilst three departments were involved in the SAR process there appeared to be no requirement for any of those involved to check the notes for third party patient data and as such, the misfiled records were not discovered. This highlighted a potentially serious failing in respect of Trust procedure and/ or staff awareness of Information Governance policies.

6. The Commissioner has taken into account the fact that in both cases a proportion of the personal data in question related to medical conditions and could potentially result in distress being caused to the individuals concerned.

7. 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.

8. 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 shall maintain and regularly assess their systems for folder redirections to ensure the personal data they retain is secure;**

2) **The data controller shall review its current asset control processes to ensure that equipment redistributed to new staff are appropriately cleared of personal data;**

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

4) **Guidance and policies around the SAR process and the requirement to remove inappropriate third party data is adequate to prevent unauthorised access to personal data; and, in particular, staff tasked with checking and redacting material from SARs receive appropriate additional training and support;**

5) **Regular mandatory refresher training in the requirements of the Act shall be provided to all staff whose role involves the routine processing of personal data; This training should include how to follow the data controller's policies;**

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: ……

Elaine Way
Chief Executive
Western Health & Social Care Trust

Dated: …….

Signed: ……

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

Dated: …….