ICO Ref: **COM0579293 and COM0641364**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Pennine Care NHS Foundation Trust
225 Old Street
Ashton-under-Lyne
Lancashire
OL6 7SR

I, Michael McCourt, Chief Executive of Pennine Care NHS Foundation Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Pennine Care NHS Foundation 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 Pennine Care NHS Foundation 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 informed of several similar data protection incidents by the data controller over a twelve month period. The number of incidents reported is of concern especially as they are repeated in nature. In some instances the Commissioner also identified delays in reporting with limited information provided even with ample time to conduct an internal investigation.

3. One of the incidents occurred in April 2015 and involved a CAMHS patient letter for a GP follow up being sent to a neighbour containing sensitive diagnosis information. On this occasion the envelope was not marked 'private and confidential' or for 'addressee only'. This incident was seen to be representative of subsequent reported data breaches to the Commissioner, where personal information was posted to the wrong person in error.

4. Information Governance concerns have been raised within the CAMHS service in general, particularly related to an inconsistency with checking patient addresses on internal systems or on correspondence before being sent. There were also identified concerns around addressees on patient records not being kept up to date. During the Commissioner's investigation into similar security incidents it was also found that administrative tasks were being undertaken by clinicians who were not clear about the correct administration procedures to protect personal data.

5. A further data security incident occurring in July 2016 involved a letter being sent to an outdated address containing confidential mental health information and its impact on the committal of an offence. Whilst the confidential letter had been returned to the service, it had been opened by an unintended recipient and could have been accessed further seeing as this was returned by a third party.

6. The investigation found that staff failed to check the Electronic Patient Record for the correct address and whilst this can be seen to be attributable to human error, there were concerns around the level of training undertaken by staff. Information Governance training was completed post incident and reliance only placed upon previous experience and college based training.

7. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of this matter. The relevant provisions of the Act are the Seventh Data Protection Principle. This Principle is set out in Schedule 1, Part I to 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 her 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 Principles in Part I of Schedule 1 to the Act, and in particular that:

(1) Procedures are put in place to ensure any reported breach of security relating to personal data is acted upon promptly and any containment and remedial measures are swiftly enforced. The Incident Reporting Policy should include provisions to train staff around reporting to timescales and to provide the most pertinent information to assist an investigation, internal categorisation and prompt remedial measures.

(2) The data controller shall ensure all processes within the CAMHS service are standardised across all teams and staff duties between administration staff and clinicians are clearly defined;

(3) To review and clarify relevant checking procedures when sending patient correspondence. This is to include procedures around patient record keeping to ensure they are kept up to date. Any related guidance should be disseminated to all staff;

(4) The completion of mandatory induction data protection training, in relation to both the requirements of the Act and the data controller's policies concerning the use of personal data, is appropriately enforced. Completion of such training including that of regular refresher training shall be recorded and monitored to ensure compliance;

Signed ……

Michael McCourt, Chief Executive of Pennine Care NHS Foundation Trust

Dated ……

Signed ……

Stephen Eckersley, Head of Enforcement

For and on behalf of the Information Commissioner

Dated ……