Ref: COM0664363, COM0644910 and COM0657647

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Cheshire West and Chester Council

58 Nicholas Street
Chester
CH1 2NP

I, Gerald Meehan, Chief Executive, for and on behalf of the Cheshire West and Chester Council, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Cheshire West and Chester Council 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 Council of Cheshire West and Chester Council 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. In February 2014, the data controller agreed to an ICO audit which was undertaken in October 2014 and following which a limited assurance rating was achieved. A follow up was undertaken on behalf of the Commissioner in June 2015, to check progress with the agreed recommendations.

3. As a result of this audit and follow up, a number of concerns relating to staff training were identified. These concerns were compounded by a series of self-reported incidents which the commissioner was advised of both during the follow up period to the audit and also thereafter. The majority of these incidents concerned disclosure in error cases and almost all involved staff who had not received data protection training. Some of these individuals were also temporary agency workers.

4. Despite agreed audit recommendations specifically related to training, which included the requirement to train all staff employed and monitor take up of such training, subsequent investigations have identified that these recommendations have not been implemented fully.

5. The Commissioner's investigation identified the general uptake of data protection training across Cheshire West and Chester Council was unsatisfactory with considerable discrepancies in the uptake of training between different service areas. Whilst overall organisational attendance at mandatory training had been at acceptable levels when the ICO conducted its consensual audit in 2014, concerns about the effective monitoring of take up had been noted on the follow up in June 2015. These concerns have continued.

6. Temporary and agency workers had also been excluded from data protection training due to the presence of a conflicting policy which stated that temporary employees are treated differently for training purposes than that of permanent employees. Additionally, the monitoring of take up of training was problematic due to the withdrawal of a compliance monitoring system which had existed previously.

7. Further data breaches reported to the Commissioner subsequent to the audit follow up have involved disclosures which had the potential to cause serious distress for those affected, including: the disclosure of an incorrect mobile phone number to an ex-partner of a data subject; allegations of historic sexual abuse being sent to an incorrect address due to the address and postcode being obtained from a Google Map search; and the Data Handling procedure, introduced following previous breaches, not being adhered to in some high risk areas as staff had not been made aware of it. Following investigations into those incidents, it was found that some staff members within these services had not received any data protection training at all.

8. Whilst the data controller has policies in place which highlight the data protection obligations of its employees, the level of overall organisational compliance with mandatory data protection training has fluctuated significantly over the last two years.

9. The latest organisational data protection training compliance figure for the year ended 2016/2017 was 61% overall, with much lower than expected attainment figures evidenced in some high risk areas such as Children and Family Services and Adult Social Care and Health.

10. 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.

11. 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 conduct a risk based training needs analysis for all roles within the organisation to ascertain the level of data protection awareness required for the role, and the frequency at which the individual should receive refresher training to ensure they are reminded of their obligations in order to prevent further security incidents. This analysis should also consider whether the training should be tailored for specific roles, and should be completed within six months of the date of the undertaking.**

2. **The data controller shall deliver mandatory data protection training in relation to both the requirements of the Act and the data controller's policies and guidance to all employees whose role involves the handling of personal data, as identified in the training needs analysis and regardless of their contractual status. This process should be completed within six months.**

3. **The data controller shall ensure that all new members of staff, responsible for the handling of personal data are given appropriate data protection training commensurate with their role upon induction.**

4. **The data controller shall ensure that mandatory refresher data protection training is undertaken at the intervals identified and as set out in the training needs analysis; such training to be refreshed annually as a minimum.**

5. **The data controller shall ensure that mandatory data protection and refresher training is monitored and enforced.**

Signed ……..

Gerald Meehan

Chief Executive

Dated ……..

Signed: ……

Stephen Eckersley

Head of Enforcement

For and on behalf of the Information Commissioner

Dated: ……