

**Data Protection Act 1998 (DPA)
Undertaking follow-up**

**Aberdeenshire Council
ICO Reference: ENF0514231**

On 20 January 2015, the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Aberdeenshire Council (AC) in relation to the undertaking it signed on 12 June 2014.

The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented. We believe that appropriate implementation of the undertaking requirements will mitigate the identified risks and support compliance with the DPA.

The follow-up assessment consisted of a desk based review of the management response which AC supplied to demonstrate the action it had taken in respect of the undertaking requirements.

The review demonstrated that AC has taken appropriate steps and put plans in place to address and mitigate the risks highlighted in the final two requirements of the undertaking:

- **(3) The data controller should ensure that attendance at data protection training sessions is fully monitored and that completion statistics are reported to relevant senior management and / or working groups, e.g. the SIRO or an information governance group. Appropriate follow up procedures should also be in place; and**
- **(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;**

by:

- recording all completion of the mandatory data protection training (whether via the ALDO e-learning system or its paper equivalent) on ALDO, ensuring that ALDO updates staff training records on the Employee Management Information System (EMIS) on a weekly basis, flagging all roles which process personal data on EMIS, automatically generating weekly reports from EMIS for a senior officer within each Service to follow-up identified staff who have failed to complete the training as required, reporting quarterly statistics to the corporate Information Security Management Group and keeping the Senior Management Team informed of relevant progress; and
- encrypting all memory sticks and laptops and smartphones, developing a corporate procedure in regard to the removal of manual records from the office and developing a reminder in Microsoft Outlook for users to select the correct recipient in instances where there are multiple employees with the same name.

The review further demonstrated that AC has taken some steps and put plans in place to address the first two requirements of the undertaking:

- **(1) The data controller shall implement its plans to provide mandatory data protection training ensuring that all staff handling personal data receive relevant training by 15 October 2014; and**
- **(2) The data controller shall, by 30 December 2014, set up a refresher programme to ensure that data protection training shall be updated and refreshed at regular intervals, not exceeding three years. The data controller should also identify departments which may require more frequent training due to the sensitivity or volume of personal data they process by this time;**

by:

- ensuring that as of 15 December 2014, 78% of staff have undertaken the mandatory data protection training; and
- ensuring the availability of refresher training via the ALDO e-learning system and a paper equivalent for staff, although refresher training is not due to commence until May 2016;

However, AC needs to complete further work to fully address these final two requirements of the undertaking, namely ensuring that:

- the remainder of staff who handle personal data, including new starters, similarly undertake the mandatory data protection training; and
- staff complete refresher training as and when required and the frequency of refresher training in the long term is clarified following the implementation of the new EMIS.

Date issued: 23 February 2015

The matters arising in this report are only those that came to our attention during the course of the follow up and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place, rests with the management of AC.

We take all reasonable care to ensure that our Undertaking follow up report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.