Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Data Protection Act 1998 (DPA)
Undertaking follow-up

Falkirk Council
ICO Reference: COM0574605

On 9 September 2016, the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Falkirk Council (FC) in relation to the undertaking they signed on 13 November 2015.

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 documentary evidence which FC supplied to demonstrate the action they had taken in respect of the undertaking requirements. This included data protection training statistics, a draft version of the Data Protection Policy which FC have subsequently ratified, meeting minutes for the Corporate Management Team, and subject access intranet guidance.

The review demonstrated that FC has taken appropriate steps and put plans in place to address and mitigate the risks which were highlighted in all of the following four requirements of the undertaking:

- **(1) Within nine months, training will be provided to all staff members who handle personal data as part of their job role. This training will be mandatory and will be refreshed annually;**

- **(2) Within six months, a process for monitoring attendance at such training, or completion of online training, will be implemented, including steps to be taken when staff members have not attended / completed training. Corporate training KPIs will be reported to and overseen by a relevant senior management group or board;**

- **(3) Within six months, improved guidance will be issued to staff members who routinely handle subject access requests. This will include details of the requirements of the Data Protection Act 1998 and how third party data should be dealt with;**

- **(4) Within six months, produce a high level Data Protection Policy, setting out the data controller's commitments to the protection of personal data and the general standards it will adhere to. This is to be communicated to all relevant staff members within one month of completion, should link to the aforementioned subject access guidance and should be referenced in the mandatory training.**

by:

- implementing a data protection and information security e-learning module, which is mandatory for all 6,800 employees (from a total workforce of 7,771) who handle personal data. FC have arranged for members of those 6,800 without routine network access to either access the e-learning or attend presentations designed and delivered by their own respective Services. FC will introduce a standardised presentation, for Services to tailor, during 2017. As of 31 July 2016, 76% of the 6,800 employees have completed the e-learning or attended a presentation; this includes localised figures of 65% for Adult Social Services and 69% for Children's Services. FC have committed to an annual refresher requirement in respect of data protection training;

- issuing monthly e-learning completion reports to Service Directors from 3 March 2016 onwards. The Corporate Management Team (CMT) have ratified key performance indicators (KPIs) in respect of the percentages of employees who handle personal data that have completed the e-learning or alternative training. The CMT will receive a report on these KPIs on 19 September 2016 and on an annual basis going forward;

- adding updated subject access guidance to the intranet at the end of May 2016, which includes a subject access process flowchart, template covering letter for subject access responses and a more general redaction note. FC rolled out this guidance to employees who routinely handle subject access requests via the quarterly FOIA / DPA Liaison Officers' Group on 30 August 2016; and

- ratifying a Data Protection Policy on 7 June 2016, which outlines a commitment to comply with the DPA, and subsequently

communicating this Policy to all staff (for example, via a reference in the mandatory training).

However, FC needs to complete further work to fully address all four requirements of the undertaking, namely ensuring that:

- the remaining 24% of the aforementioned 6,800 and (on an ongoing basis) all new employees who will also handle personal data, either complete the e-learning or attend the alternative presentation. FC should also ensure that all employees who handle personal data undertake refresher data protection training annually, as planned;

- FC regularly generate completion reports in respect of the presentations for employees without network access and periodically monitor these at a corporate, as well as at Service, level. FC record the e-learning, but not attendance at the presentations, on the Human Resources system used for reporting. Services must manually cross-reference e-learning completion reports against other records for training undertaken by employees without network access;

- subject access guidance and / or policies which are intended for employees who routinely handle subject access requests, closely align with the specific process for handling such requests in practice at FC, as the current intranet guidance incorporates more general considerations; and

- the Data Protection Policy includes a reference to the subject access guidance and / or policies.

Date Issued: 9 September 2016.

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 FC.

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.