

Introduction

The ICO was invited to conduct a data protection audit by the Council. The audit took place in spring 2014. The audit covered three main areas:

- Records management (manual and electronic)
 - The process in place for managing both manual and electronic records containing personal data.
- Training and awareness
 - The provision and monitoring of staff data protection training.
- Subject Access Requests
 - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.

Findings

The ICO audit made 49 recommendations to the Council, and gave a rating of "Limited Assurance" for Records Management and Training and Awareness and a rating of "Reasonable Assurance" for Subject Access Requests. This translates into an overall rating of Limited Assurance.

Current status

80% of all recommendations are now complete, with the remaining actions almost complete.

The ICO recommended that the Council continues to work towards full implementation of their recommendations. In particular

- The appointment of a corporate Records Manager to take the lead for records management
 - The business case for the role was approved during 2015
 - An advert is currently live for the position
- The delivery of specialised training for specialised roles
 - This was provided in June 2015 by the National Archives.
 - A revised Data Protection course has been released for all staff
 - Councillors have received dedicated briefing sessions
 - Further sessions will take place after the election

In addition here was an essential requirement to identify all of the council's information assets, and create asset registers with which to manage those assets and all of the risks associated with them.

This work is now underway, and is integral to the Council's information management strategy, which will introduce further improvements in this area for the council.

Conclusion

On completion of all of the recommendations, which have a target of Q2 2016, the Council will be in a far stronger position than in 2014 with a mature approach to managing all information assets, and full clarity on their location, people that are authorised to use them, and any associated risks.