Leeds CITY COUNCIL

Report author: Andrew Nutting
Tel: 07891 276168

Report of Assistant Chief Executive (Citizens and Communities) and Deputy Chief Executive*

Report to Corporate Governance and Audit Committee

Date: 21st January 2014

Subject: Report of the Information Commissioner's Office following a Data Protection Audit conducted across the Council

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☐ Yes	☒ No
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

Summary of main issues

1. The council agreed to the Information Commissioner's Office (ICO) undertaking a consensual data protection audit between 1st and 3rd October 2013.

2. The primary purpose of the audit is to provide the ICO and the council with an independent opinion of the extent to which the council is complying with the Data Protection Act 1998 (DPA98) and highlight any areas of risk to compliance.

3. This report provides Corporate Governance and Audit Committee with background information about the audit, together with a copy of the final report, assessment and recommendations for improved practice from the ICO

4. The audit concluded that the council is providing a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance.

Recommendations

5. Corporate Governance and Audit Committee is asked to consider the contents of this report and note the level of assurance the council has provided the Information Commissioner's Office in respect of its processes and procedures for delivering data protection compliance.

*The role of Senior Information Risk Owner (SIRO) for the council is to change from Assistant Chief Executive (Citizens and Communities) to the Deputy Chief Executive on 7th January 2014. However the audit work was completed whilst the Assistant Chief Executive was the SIRO.

1 Purpose of this report

1.1 The council agreed to the Information Commissioner's Office (ICO) undertaking a consensual data protection audit between 1st and 3rd October 2013.

1.2 The purpose of this report is to ensure that Corporate Governance and Audit Committee have sight of the recommendations contained within ICO audit report and consider their implications for the council.

2 Background information

2.1 The council agreed to the ICO undertaking a consensual data protection audit between 1st and 3rd October 2013. The primary purpose of the audit was to provide the ICO and the council with an independent opinion of the extent to which the council is complying with the Data Protection Act 1998 (DPA98) and highlight any areas of risk to compliance.

2.2 The ICO have produced a report detailing the audit findings, an assurance rating of the council and a series of recommendations for improvement. The overall conclusion reached by the report is that the council can provide the ICO with a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance.

2.3 The ICO report is attached to this report as Appendix One to provide members of the Corporate Governance and Audit Committee with details about the level of assurance provided and information about the actions proposed to improve processes and procedures to comply with the DPA98.

3 Main issues

3.1 The Information Commissioner is responsible for enforcing and promoting compliance with the DPA98. Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller (the council). This is done through a consensual audit.

3.2 The council were the subject of ICO enforcement action in 2012 with both an Undertaking and a Civil Monetary Penalty issued for separate data protection breaches. Subsequent to the payment of the Civil Monetary Penalty and completion of work on the Undertaking, the council agreed to a request by the ICO for them to undertake a consensual audit of our practice and procedures for processing personal data.

3.3 The audit was conducted between the 1st and 3rd October during which time two auditors interviewed staff across specific areas of the council. These areas had been previously agreed at an introductory meeting on 25th June to discuss the scope of the audit, and were focussed on those services processing high risk information and those areas responsible for information management security and policy. The scope of the audit was limited to how the council manages manual and electronic records containing personal data and the security arrangements for personal information.

3.4 Following the audit and further consultation with the Corporate Information Governance Team, the ICO published a report on 29th November 2013, which concluded that the council is providing a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The reasonable assurance is the second highest ranking out of four the ICO use to assess organisations. The audit has identified some scope for improvement in existing arrangements and has proposed a series of recommended actions within the report to reduce the risk of non-compliance with the DPA98.

3.5 There are thirty-two recommended actions, to which the council has accepted twenty-seven in their entirety, and partially accepted the remaining five recommendations. The council proposed amendments to each of the partially accepted recommendations and these amendments have subsequently been accepted by the ICO. Details about each amendment are located within the ICO report at reference point's **a22**; **a39**; **a44**; **b32**, and **b48**.

3.6 The council has agreed to report back to the ICO by 8th September 2014 in respect of progress in implementing actions against each recommendation. The Data Protection Audit Working Group, set up to coordinate arrangements for the audit, will remain in place to monitor progress against each recommendation. It should be noted that there were no real surprises contained within the ICO report and that the council had already started work on a number of the recommendations contained within the report.

3.7 As part of the audit process the ICO request permission to publish an Executive Summary of the audit findings on their website. The council had ten days from publication of the report to provide this approval, otherwise the ICO website would be updated to say that the audit took place but permission to publish was withheld. Given that the audit findings were relatively favourable to the council, the council's Senior Information Risk Officer (SIRO) took the view that it was appropriate to provide approval for the ICO to publish the Executive Summary on their website. A copy of this Executive Summary is provided at Appendix Two.

4 Corporate Considerations

4.1 Consultation and Engagement

4.1.1 This was a consensual audit undertaken on the council at the request of the ICO and no formal consultation was necessary or required. However, the undertaking of the audit required engagement with a wide cross-section of officer stakeholders from within the council, all of whom were kept informed about the audit process throughout, and contributed to the eventual outcomes detailed in the ICO audit report.

4.2 Equality and Diversity / Cohesion and Integration

4.2.1 Equalities and diversity is an integral and prerequisite consideration within the Data Protection Act and due regard has to be made to Schedule two and three of

the legislation when processing personal data consisting of information relating to the racial or ethnic origin of a data subject.

4.3 Council policies and City Priorities

4.3.1 Implementation of improvements to the council's data protection practice and procedures will provide citizen confidence in the council's ability to process their personal data in a safe, secure and reliable manner, thereby ensuring that council plans and strategies, particularly the Children's and Young Peoples Plan and the Health and Well Being City Priority Plan, which will rely on effective sharing of personal data, can be delivered compliantly and effectively.

4.4 Resources and value for money

4.4.1 The ICO's audit report makes some recommendations with revenue implications for the council. Notably there is a recommendation that the council's Corporate Information Governance Team responsible for producing effective information governance training materials have a permanent training resource within the team. A further recommendation requires members of the Corporate Information Governance Team are suitably qualified to enable them to carry out their role effectively.

4.4.2 Budget implications contained within the audit report are being considered as part of determining the budget for 2014/15.

4.5 Legal Implications, Access to Information and Call In

4.5.1 There are no legal implications from this report.

4.5.2 There are no restrictions to access to information contained in this report.

4.6 Risk Management

4.6.3 The risk associated with not implementing information governance policies, procedures and practice across the Council leaves the organisation more susceptible to breaches of legislative, regulatory and contractual obligations, affecting the confidence of its citizens, partners, contractors and third parties when handling and storing sensitive and protectively marked information.

4.6.1 The risk associated with not implementing the recommendations and subsequent action plan contained within the audit report leaves the council open to criticism from the ICO, reputational damage and the possibility of further Monetary Penalty Notices being issued.

5 Conclusions

5.1 The Data Protection Audit has provided the council with the opportunity to use the ICO's experienced, qualified staff to provide an independent assurance of data protection compliance. It has also helped to independently raise staff awareness of data protection and demonstrated the council's commitment to, and recognition of, the importance of data protection.

5.2 The purpose of the audit was to provide the ICO and the council with an independent assurance of the extent to which the council within the scope of the audit is complying with the DPA98. The overall conclusion is that there is a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA98, and these will be addressed through implementing a number of recommendations contained within the report through delivery of an action plan by 8th September 2014.

6 Recommendations

6.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and note the level of assurance the council has provided an independent regulator in respect of the council's processes and procedures for delivering data protection compliance.

6.2 Corporate Governance and Audit Committee will receive a further report in July 2014 outlining the council's progress in implementing the recommended actions for improving compliance contained within the ICO report. Furthermore, the assurances provided by this independent audit will feed into the assurances provided for the Annual Governance Statement.