Audit and Procurement Committee   25 February 2019

Name of Cabinet Member:
Cabinet Member Policy and Leadership, Councillor Duggins

Director Approving Submission of the report:
Director of Finance and Corporate Services

Ward(s) affected:
None

Title:
Information Commissioner's Office – Data Protection Audit Progress Report

Is this a key decision?
No

Executive Summary:

In November 2017, the Information Commissioner's Office (ICO) carried out a data protection audit into the City Council's governance arrangements, training and awareness and data sharing arrangements. The ICO issued its final report in February 2018 which included a range of recommendations. The outcome of the audit and the Council's action plan were reported to the Audit and Procurement Committee later that month and this report sets out progress over the last year against the agreed actions.

Recommendations:

Audit and Procurement Committee is recommended to:

1)   Note the progress made in response to the recommendations arising from the audit

2)   Make any recommendations to the Cabinet Member for Policy and Leadership who is the portfolio holder for information management and governance

List of Appendices included:
Appendix 1: Progress against action plan

Background papers:
None

Other useful documents
Briefing note to Audit and Procurement Committee Information Commissioner's Office – Data Protection Audit November 2017, 19 February 2018.

Has it been or will it be considered by Scrutiny?
No

Has it been or will it be considered by any other Council Committee, Advisory Panel or other body?
No

Will this report go to Council?
No

Report title: Information Commissioner's Office – Data Protection Audit Progress Report

1.   Context (or background)

1.1   In October 2015, the Information Commissioner's Office (ICO) carried out a data protection audit into the City Council's governance arrangements, training and awareness and data sharing arrangements. In addition to meeting with officers responsible for corporate arrangements, it spoke to staff in Children's Social Care and the Revenues and Benefits service. The audit concluded that there was "very limited assurance that processes and procedures are in place and deliver data protection compliance." It made recommendations for the Council to strengthen its arrangements which the City Council implemented as part of a significant programme of work to strengthen its approach to information governance. The Audit and Procurement Committee has received regular reports on progress against the ICO's recommendations since then.

1.2   In November 2017 the ICO revisited the authority to carry out a further data protection audit. It followed the same scope, looking at governance arrangements, training and awareness and data sharing arrangements corporately and in Children's Social Care and the Revenues and Benefits service. As previously, the audit provided a snapshot of assurance levels at a moment in time rather than specifically looking at the direction of travel or progress since the previous audit.

1.3   In commenting on the progress made by the City Council, the ICO's Lead Auditor, who was a member of the ICO team for both audits wrote that "*in our view, comparison between the assurance ratings strongly reflects on the work undertaken at CCC since our original audit. … This demonstrates a clear improvement and progress at an individual, as well as an overall, level*".

1.4   The ICO report made 141 detailed recommendations for the Council to consider, some of which were duplicated. Of these recommendations:

- 18 recommendations were rejected as arrangements were already in place to address the issues raised;
- 32 had already been completed as they proposed only very minor amendments to processes or documents;
- 91 fell into three main areas where the Council had further work to do. Many of them supported existing planned action, particularly work being undertaken to ensure the City Council was ready for the introduction of the General Data Protection Regulation in May 2018.

1.5   The outcomes of the audit and the Council's consolidated action plan in response to the ICO's recommendations were reported to Audit and Procurement Committee in February 2018 and progress against the action plan is set out in Appendix 1. The main areas of focus of the three areas covered in the audit and action plan, together with a summary of progress are set out below.

1.6   **Data Protection Governance:**

1.6.1   Summary of position at February 2018: Since the initial audit, the City Council had made significant progress in the development of policies, roles and responsibilities to ensure data protection governance arrangements were clear and consistent. This was set out in the Information Governance Handbook which is the single source of information on Information Governance arrangements and is regularly reviewed and updated. The Council had also developed its approach to information risk management and put in place policies, procedures and oversight to ensure that risks to information are managed

effectively. Information governance was highlighted on the corporate risk register, appropriate roles and responsibilities had been designated and risk management had improved. However, work was still required to populate and review information risk registers.

1.6.2 Summary of progress at February 2019: This was the area where the most recommendations were made and the majority have been completed. Policies, roles and responsibilities continue to be reviewed and updated. A number of actions remain in progress and the most significant area outstanding relates to information asset and risk management. Information Asset Owners and Managers have received training on identifying information assets, the requirement to have these assets documented and asses risk on an annual basis as a minimum but this needs ongoing support from the Information Governance Team to assist the Information Asset Owners in ensuring the completion and accuracy of the registers. The update of the information asset register and completion of information risk registers is a priority.

1.7 **Training and Awareness:**

1.7.1 Summary of position at February 2018: The ICO audit recognised the considerable work that had gone into strengthening data protection training and awareness raising across the Council since the previous audit and this was reflected in the reasonable assurance rating given to this area. This included the work undertaken by the Information Management Strategy Group to ensure that appropriate training, including the mandatory training for all staff, was carried out which was highlighted as good practice. However, the audit report recommended the introduction of a comprehensive training strategy to address the Council's approach to general and specialist training. This was accepted and was in preparation at the time of the report.

1.7.2 Summary of progress at February 2019: The actions identified under this heading have been completed and a comprehensive Training Strategy was approved by Information Management Strategy Group in April 2018. Over the next few months the Strategy will be reviewed and updated to reflect developments nationally, elsewhere in local government and learning from the first year of its implementation.

1.8 **Data Sharing:**

1.8.1 Summary of position at February 2018: The Council's data sharing arrangements had improved significantly since the time of the initial audit and this part of the report included the fewest number of recommendations. The recommendations that were made focussed on improving the consistency and robustness of arrangements and these were accepted.

1.8.2 Summary of progress at February 2019: The majority of the actions identified under this heading have been completed. The Information Governance Team has continued to work with service areas to improve data sharing awareness and activity. Much of this activity was carried out through the development of Records of Processing Activities and/or the review and preparation of Privacy Notices carried out to support the implementation of GDPR.

2. **Options considered and recommended proposal**

2.1 Audit and Procurement Committee is recommended to note the progress made in response to the recommendations arising from the audit as set out in Appendix 1 and make any recommendations to the Cabinet Member for Policy and Leadership who is the portfolio holder for information management and governance

3.   Results of consultation undertaken

3.1   Not applicable.

4.   Timetable for implementing this decision

4.1   Timescales are set out in the action plan and commentary.

5.   Comments from Director of Finance and Corporate Services

5.1   Financial implications

There are no specific financial implications arising from this report.

5.2   Legal implications

There are no specific legal implications arising from this report.

6.   Other implications

6.1   How will this contribute to the Council Plan (www.coventry.gov.uk/councilplan/**)?**

Ensuring effective arrangements are in place for data protection contributes to high standards of information governance and contribute to the openness and transparency of the Council's decision making and commitment to continuous service improvement and equality.

6.2   How is risk being managed?

Information risk management is a key part of data protection governance and is linked to the Council's overall risk management process.

6.3   What is the impact on the organisation?

As set out in paragraph 6.1.

6.4   Equalities / EIA

As set out in paragraph 6.1.

6.5   Implications for (or impact on) the environment

None

6.6   Implications for partner organisations?

None

Report author(s):

Name and job title:
Adrian West
Members and Elections Team Manager

Directorate:
Place

Tel and email contact:
Tel: 024 7697 1007
Email: adrian.west@coventry.gov.uk

Enquiries should be directed to the above person.

Contributor/approver name	Title	Directorate or organisation	Date doc sent out	Date response received or approved
Contributors:				
Sharon Lock	Head of Information Governance	Place	11 February 2019	13 February 2019
Lara Knight	Governance Services Officer	Place	11 February 2019	13 February 2019
Names of approvers for submission: (officers and members)				
Finance: Paul Jennings	Finance Manager (Corporate Finance)	Place	11 February 2019	12 February 2019
Legal: Sarah Harriott	Corporate Governance Lawyer, Legal Services	Place	11 February 2019	12 February 2019
Director: Barry Hastie	Director of Finance and Corporate Services	Place	11 February 2019	15 February 2019
Members: Cllr Duggins	Cabinet Member for Policy and Leadership	Place	11 February 2019	11 February 2019

This report is published on the council's website:
www.coventry.gov.uk/councilmeetings

Progress against action plan

Data Protection Governance

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
1	A9, A11	Review Job descriptions in the Information Governance Team as part of the planned restructure following recent staff and organisational changes. We have in the meantime clearly allocated line management responsibility.	May-18	Members and Elections Team Manager	Complete. Job descriptions reviewed as part of a restructure of the Information Governance Team which has been implemented. All posts filled from January 2019.
2	A26a, A28a, A90, A91, A94	Make available templates for policies, procedures and guidance ensuring document control is included. Create a policy index to signpost to the single version of each policy as prescribed by the Information Governance handbook and incorporate date of review to ensure clarity and regular review.	Apr-18	Records Manager	In progress – Document control has been introduced within Information Governance and associated policies. The rollout of document control, development of a policy index and annual review of policies across the Council will form part of the Records Management activities in the Information Governance Team's workplan.
3	A27, A34a, A36	Fully implement the Information Risk Management Process, including the completion of the Information Risk Registers by Information Asset Owners, regular review of the Information Asset Register and the process for providing formal assurance to the Senior Information Risk Owner on relevant information assets. The duties responsibilities for risk escalation are already detailed within the Council's Risk Management Policy, Strategy and Framework. The Information Asset Register and Information Risk Register will then be subject to annual review.	Jul-18	Head of Information Governance	In progress - Information Risk Management guidance is available to all on the Information Governance Handbook. The risk register is incorporated into the Information Asset Register. The annual review is not complete and the Information Governance Team will work with Information Asset Owners and Managers to ensure completion by end of April 2019 and provide annual assurance to the Senior Information Risk Officer.

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
4	A28b	Update the risk management framework to cross-reference to the Information Risk Policy and Registers. The Risk Management Policy and Strategy will be updated during the next review cycle.	Mar-18	Insurance Manager	In progress. This will be considered during the next review cycle.
5	A31	The Senior Information Risk Owner is to nominate an alternative Officer to act as Information Asset Owner for his services	Jul-18	Senior Information Risk Owner	Complete.
6	A37	Implement and raise awareness of a formal and documented Information Security Incident Management Policy (building on the existing draft procedures), which outlines objectives, key roles and responsibilities, a process flowchart and detailed guidance as to the various stages of the incident management process	Mar-18	Head of Information Governance	Complete. Data Breach Incident response plan is published on the Information Governance Handbook Handbook and links to the Data Handling Policy, Data Protection Policy and Data Breach Incident Response Process Map.
7	A52, A68	Consider the best method of linking the Corporate Risk Register and the Information Risk Register/Information Asset Register to ensure that information risks can be escalated appropriately and consistently as required.	Jul-18	Head of Information Governance / Insurance Manager	Complete. The Risk Management framework is designed to allow identification and escalation of risks as appropriate. Reports to senior management, follow up with specific service areas and other communications ensure issues escalated to the appropriate level.
8	A54, A55a, A55b, A56, A58	Ensure that the contract template and live contracts consistently incorporate the requirement for data processors to act only on their instruction. This will be completed as part of our preparations for GDPR	May-18	Information Governance Lawyer/IGT	Complete. Contract templates have been reviewed based on the Central Government Policy Procurement Practice Note to ensure that any new contracts going forward incorporate the new terms required by GDPR, namely that processors act under instruction from the City Council as data controller and provide written assurances that they have the

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
					technical and organisational measures to keep information safe. A generic variation clause incorporating GDPR into existing contracts has been sent in respect of existing contracts by Procurement.
9	A59, A63	Draft, implement and raise awareness of a formal and documented Privacy Impact Assessment Policy, which outlines objectives, key roles and responsibilities, a process flowchart and detailed guidance as to the various stages of the PIA process. Ensure that this policy is cross-referenced within other associated data protection policies.	May-18	Head of Information Governance	In progress. Draft Policy complete and scheduled for approval at the next Information Strategy Group. The Information Governance Team already applies the policy, including when supporting internal customers with Privacy Impact Assessments.
10	A66	Ensure that the Privacy Impact Assessment register includes hyperlinks to copies of the individual Privacy Impact Assessments where possible.	Aug-18	Head of Information Governance	Complete.
11	A74	Consider aligning the Council to external standards to improve the effectiveness of data handling controls, for example by consistently benchmarking data protection policies against these.	May-18	Information Management Strategy Group	Complete. Information Governance/ Data Protection policies are devised in accordance with ICO guidance and/or templates and appropriately tailored to City Council.
12	A76	Establish a comprehensive range of formal documented data protection Key Performance Indicators, report against these on an ongoing basis and ensure that the audience for this reporting includes the Corporate Leadership Team and Information Management Strategy Group, in order to facilitate a high-level view of organisational performance.	Jun-18	Information Management Strategy Group	Complete. These are standing agenda items on Information Management Strategy Group meeting agendas.

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
13	A81, A82, A87, A88, A92, A93, A100	Undertake an annual review of all Information Governance Policies within the Information Governance Handbook and ensure consistent branding. This will need to also consider changes for May 2018 and the introduction of GDPR.	May-18	Records Manager	Complete. This is part of annual review and was carried out in readiness for GDPR.
14	A83	Amend the Information Security Management Policy to outline the responsibilities of individuals and teams and / or groups with core information security roles and provide an overview of key aspects of information security such as incident management and physical security. Amend the Data Handling Policy to provide content in regard to corporate data handling requirements.	Apr-18	Head of Information Governance	Complete. These are available in the Information Governance Handbook.
15	A96, A106	Consider the best method of ensuring that communications are received, read and understood by using GovDelivery or similar tools to provide data and evidence of users accessing material that is shared.	Dec-18	Head of Communications	In progress. The GovDelivery system provides the facility to evidence the number of employees accessing emails, links and policies but this has not been utilised by Information Governance. This will be built into the communications plan and performance review process for the coming year.

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
16	A99	Develop a more in-depth series of checks in respect of the main themes of data protection compliance such as information security and records management, either within the same or dedicated checklists, and periodically rotate between conducting such checks. For example, checks in regard to information security could include physical access to and within Council buildings, access to manual records storage in open office areas, adherence to clear desk and screen, and the disposal of electronic hardware and manual records.	Aug-18	Head of Information Governance	In progress. A new spot check annual programme is in place for the Information Governance Team to carry out during the coming year. Work is being undertaken with Internal Audit to ensure activity aligns with the Internal Audit programme and information is captured effectively.

Training and Awareness

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
1	A7, A61, A78, B2, B10, B14, B18, B22, B30, B35, B40, B41, B42, B43, B50, B53, B72	Compile a training strategy to formally document the approach taken to training. The strategy will contain: - Training objectives - Training methods - Available courses and the mix of mandatory, specialist and non-mandatory training. - Alternative training methods for non-networked, agency and 3rd party staff - How training will be evaluated - How take up is monitored - Roles and responsibilities in ensuring compliance	31st March 2018	Programme Manager (Transformation)	Complete.
2	B2, B4, B5, B74, B78	Update the Information Governance Handbook, and suite of Data Protection policies to include the roles and responsibilities of the Senior Information Risk Owner, Data Protection Officer and Information Management Strategy Group in relation to training	31st March 2018	Programme Manager (Transformation)	Complete.
3	B21	Utilise functionality in the recently implemented online learning system (Me-Learning), to enable feedback to be provided by trainees on course material and to use that feedback to inform future training provision.	31st March 2018	Programme Manager (Transformation)	Complete.
4	B26	Include further detail on Subject Access Requests and Cyber-Security into the mandatory training.	31st March 2018	Programme Manager (Transformation)	Complete. Cyber security has been incorporated into the mandatory training for all staff. Staff involved in dealing with SARs are required to

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
					carry out a specific training module. Consideration will be given in next review of training strategy to widening this to others.
5	A103, A104, B32, B36	Ensure that induction checklists consistently document the requirement for mandatory training to be completed, with links to the policies and training. This is to be extended to all staff including temporary and agency staff.	31st March 2018	Programme Manager (Transformation)	Complete. Induction Checklist for Agency Worker includes Data Protection but approach will be reviewed as part of next review of the Training Strategy.
6	B34	Ensure that agency staff have clear instructions on how to access the newly implemented online learning platform (Me-Learning)	31st March 2018	Programme Manager (Transformation)	Complete.
7	B54	Finalise a communications plan which covers the requirements for training to be completed, together with periodic communications covering Data Protection awareness themes.	31st March 2018	Programme Manager (Transformation)	Complete. Communications plan underpinned effective rollout and update of revised training ahead of the implementation of GDPR. Review of training plan and associated communications plan scheduled for the next meeting of the Information Management Strategy Group.

Data Sharing

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
1	c2, a26a, a92	Create and enforce use of a Policy Template, ensure it states that policies are subject to annual review and contains the appropriate document control.	May-18	Records Manager	In progress. Complete for Information Management and will be embedded across the Council as part of the planned Records Management project.
2	c8	Enforce the process that requires staff that are involved in one-off data sharing undertake the relevant training	Mar-18	Information Governance Team/Senior Management	In progress. Training for staff dealing with Subject Access Reviews is due for review and the Information Governance Team will explore the most effective method of delivery.
3	c10	Consider merging the Privacy Policy and the Corporate Privacy Statement, make available from the website homepage and that it provides links to the Current Data Sharing agreements	May-18	Information Governance Team/Information Management Strategy Group	Complete. Corporate Privacy Notice revised and available on website.
4	c12	Implement a formal sign-off process for and register of, Privacy Notices, to ensure corporate oversight for the fair processing information provided	Jun-18	Senior Information Governance Officer	Complete.
5	c14,	Review the Data Sharing training and incorporate new requirements under GDPR.	May-18	Senior Information Governance Officer	Complete.
6	c19	Carry out a review of the Privacy Impact Assessment template; ensure template specifies which Data Protection Act condition for processing or exemption applies.	Jun-18	Senior Information Governance Officer/ Information Governance Team	Complete.

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
7	c22, c30, c31, c32, c33, c34, c37, c13	Ensure that all Data Sharing Agreements: - Include statements of compliance signed by senior management of each participating Data Controller. - Consistently detail whether information to be shared is fact or opinion. - Consistently outline a requirement for the sender of the information to inform recipients when data has been amended or updated. - Implement processes to ensure the information received and being shared as part of a DSA is accurate and up to date. - Amend DSA template to facilitate compliance to the fifth principle of the Data Protection Act. - Contain consistent requirements for the secure disposal of information in line with Retention & Disposal Schedule. - Include a requirement for 3rd parties to notify the Council when information is deleted. - Include a clause stating how a Data Breach should be reported and a specific timeframe given. - Consistently provide details of how fair processing information will be given to individuals	May-18	Senior Information Governance Officer	Complete.
8	c23	Approve the MASH Partnership Agreement as soon as possible.	Feb-18	Senior Information Governance Officer	Complete.
9	c26	Review all Council contract templates in preparation for GDPR to ensure their compliance with the Regulation. Undertake a review of existing contracts.	May-18	Information Governance Lawyer/Contracts Manager	Complete. Contract templates have been reviewed based on the Central Government Policy Procurement Practice Note to ensure that any new contracts going forward incorporate the new terms required by GDPR,

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner	Progress
					namely that processors act under instruction from the City Council as data controller and provide written assurances that they have the technical and organisational measures to keep information safe.
10	c42	Ensure that the Information Management Strategy Group have access to central log for one-off disclosures.	May-18	Information Governance Team/ Information Management Strategy Group	No progress. Central log in place and managed by Information Governance Team as part of the Subject Access Request Register. It is not appropriate for the wider Group to have access to this and options to strengthen corporate oversight will be considered by the Group by April 2019.