Coventry City Council

Public report
Audit and Procurement Committee

Audit and Procurement Committee — 24th July 2017

Name of Cabinet Member:
Cabinet Member for Policy and Leadership - Councillor Duggins

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

Ward(s) affected:
None

Title:
2016/17 Information Governance Annual Report

Is this a key decision?
No

Executive Summary:

Data Protection and transparency legislation are identified as important factors in the Council's Information Management Strategy. This report highlights the Council's performance in relation to handling requests for information, managing data protection security incidents and completing data protection training demonstrating the Council's commitment to the strategy and compliance with relevant legislation.

Compliance and performance have improved from last year's position following the Information Commissioner's Office (ICO) audit report received in 2016 and recommendations that have been implemented. There is still work to be done to embed these actions within the Council in order to gain full compliance. The General Data Protection Regulation (GDPR) comes into force on 25th May 2018 and will introduce major changes to the Data Protection Act 1998 (DPA). This is an additional challenge that will introduce stricter rules around the way we capture, use and retain personal information and will attract higher financial penalties for non-compliance.

Under the Freedom of Information Act 2000 (FOIA) the Council is required to respond to requests for information it holds from members of the public subject to any exemptions that may apply. The Environmental Information Regulations 2004 (EIR), require Public Authorities to consider disclosure of environmental information under EIR rather than FOIA. Both FOIA and EIR encourage proactive publication of information however the EIR provides fewer grounds for public authorities to withhold information.

The DPA requires the authority to process personal data in accordance with the principles of the Act, which includes providing access to information the Council processes about them, subject to any exemptions. DPA security breaches occur when there is unlawful or unauthorised processing of personal data, or where there is accidental loss, damage or destruction to personal data. The Council is required to report serious breaches to the ICO. It is also required to have in place

technical and organisational measures to minimise occurrence of such incidents. DPA training is one of the organisational measures the Council is required to have in place.

The Information Commissioner's Office (ICO) oversees FOIA, EIR and DPA compliance, promotes good practice and deals with complaints from members of the public who are not satisfied with the response they receive. The ICO also investigates data protection breaches reported to them and can exercise enforcement powers that include civil monetary penalties. This report provides an overview of the number of requests for information received under the FOIA, EIR and DPA and the completion rate, outcome of internal reviews and complaints made to the ICO during 2016/17. This report also covers data protection security incidents reported and DPA training completed.

Recommendations:

The Audit & Procurement Committee are requested to consider and note:

(1) The Council's performance on Freedom of Information, Subject Access and other Data Protection Act requests. This covers the number of responses within statutory time limits, outcome of internal reviews and number and outcome of complaints made to the ICO.

(2) Data security incidents reported. This includes the number, nature and risk level.

(3) DPA training completed. This covers the number of employees that have completed the training.

List of Appendices included:
Annex A – Number of FOI/EIR requests received and completion rates in the last 3 years
Annex B – Number of Subject Access Requests received and completion rates in the last 3 years
Annex C – Nature of Data protection security breaches reported and severity in 2016/17

Other useful background papers:
None

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

Page 3 onwards
Report title: 2016/17 Information Governance Annual Report

1. Context (or background)

1.1 The Information Management Strategy Group (IMSG) oversees the Council's performance in relation to handling requests under the FOIA, EIR and DPA. This is part of monitoring compliance with relevant legislation as stated in the strategy. The Information Governance Team (IGT) coordinates requests received. The team also manages data protection security incidents reported to them by recording, investigating where necessary and recommending actions to be taken based on the risk level.

1.2 The Council is obliged to respond to information requests under FOIA/EIR within 20 working days, subject to relevant exemptions. The Code of Practice, issued by the Secretary of State for Constitutional Affairs under Section 45 of FOIA, requires public authorities to have a procedure in place to deal with complaints in regard to how their requests have been handled. This process is handled by the IGT as an FOI/EIR internal review.

1.3 After an internal review has been completed an applicant has a right to complain to the ICO for an independent ruling on the outcome. Based on the findings of their investigations, the ICO may issue a Decision Notice. The ICO also monitors public authorities that do not respond to at least 90% (previously 85%) of FOI/EIR requests they receive within 20 working days.

1.4 The DPA provides individuals with the right to ask for information that the Council holds about them. These are also known as Subject Access Requests (SARs). The Council should be satisfied about the individual's identity, have sufficient information about the request and receive the statutory £10 fee before it can respond. SARs have to be completed within 40 calendar days.

1.5 There is no requirement for the Council to have an internal review process for SARs. However, it is considered good practice to do so. Therefore, like with FOIA/EIR requests, the Council informs applicants of the Council's internal review process. However, individuals may complain directly to the ICO if they feel their rights have not been upheld.

1.6 The Council also receives "one-off" requests for personal information from third parties including the police and other government agencies. The IGT maintains a central log that includes exemptions relied on when personal data is shared with third parties. The IGT gives advice and assesses whether the Council is allowed to disclose the information or not.

1.7 Data breaches reported to the IGT vary in severity based on the nature of the data compromised and the impact of the breach on the data subjects or the people whom the information is about.

1.8 This report covers how the Council handles requests received under FOIA, EIR and DPA. It outlines the number of requests received, proportion of responses completed within the set timescales and outcomes of internal reviews and complaints made to the ICO during 2016/17. Details on the number of data protection security incident reported and DPA training completed by Council employees are also included.

1.9 **Freedom of Information and Environmental information Regulations**

1.9.1 FOI/EIR performance in the last 3 years.
1374 FOI/EIR requests were received in period 2016/17, compared to 1329 requests received in the previous year. The Council responded to 68% of FOIA/EIR requests within 20 working days in 2016/17 compared to 60% for the previous year. This improvement may be as a result of improved processes; a new system has been put in place that notifies the information owner of a received request when the request is logged by IGT. Our figure is below the required level of 90% by the ICO, however we continue to make progress. See Annex A

1.9.2 There were15 requests for internal reviews in the year 2016/17 compared to 18 in the previous year. The Council responded to 12 of these with the following outcomes:

- 5 were not upheld - exemptions applied were maintained and no further information was provided
- 3 partially upheld - further information provided
- 4 upheld - information provided
- 3 remain under consideration.

1.9.3 Three complaints were referred to the ICO. The reasons and outcomes for these were:

- Response not received to a request for an internal review; internal review processed
- Initial response to request not received; response provided
- Requester stated they had not received a response to their internal review; response re-issued.

1.10 **Data Protection Act Requests**

1.10.1 The Council received 144 valid SARs during the course of 2016/17, compared to 93 in the previous year. There was an improvement in the response rate to SARs 112 (68%) were completed within 40 calendar days compared to 53% in 2015/16. The Council still receives requests relating to social care that are complex to deal with and take a long time to complete. Summary of the number of requests received performance in the last 3 years is shown in Annex B.

1.10.2 The Council received three SAR internal review applications in the course of the year, that were all partially upheld and additional information was disclosed. There were three SAR complaints referred to the ICO. In all three, Council had taken more than 40 calendar days to respond. In one of the complaints, the Council did not hold the required information and the complainant was referred to the relevant organisation. In another complaint, there was inconsistency in the way the information was redacted and more information was required. Following the complaints there has been an improvement in the way SARs are processed this includes a closer monitoring of the process by the IGT and a quality check of responses before disclosure.

1.10.3 The new General Data Protection Regulations (GDPR) that will be in effect from May 2018 will require the Council to respond to SARs within one calendar month (and 2 calendar months for complex requests). Under the GDPR, the Council will no longer be able to charge a £10 fee for SARs. The Council can be fined a maximum of 20 million Euros for not meeting the deadlines or providing insufficient information to the requester. The IGT has recently rolled out an eLearning training aimed for employees that handle SARs.

1.10.4 Under Section 29 of the DPA the police and other agencies can request for personal information for the purposes of prevention and detection of crime. Other DPA exemptions exist where the organisations can disclose personal data in exceptional situations. 398 'one-off' requests were logged on the central register managed by the IGT. 340 (95%) of these requests have been closed on the central register. IGT responded to a majority of these and others were allocated directly to specific service areas to respond.

1.11 **Data Protection Security Incidents**

1.11.1 The Council's Information Management Strategy sets out the need to protect information from theft, loss, unauthorised access, abuse and misuse. The importance of this is to reduce the risk of data breaches or financial loss incurred through non-compliance with key legislation such as the DPA. It is good practice to report on information incidents and breaches.

1.11.2 The Data protection security incident reporting process promotes an awareness of the need to handle personal information securely. The investigation and mitigation element serves as a reminder/refresher of ensuring that there are sufficient controls in place to ensure that personal information is secure. It further allows us to 'learn from our mistakes' and prevent serious breaches that may cause harm to individuals and the Council.

1.11.3 There are continuous improvements being made to the data security breach management process that is being aligned to the new Information Risk Management Policy, approved in March 2017. The new Information Asset Register identifies designated Information Asset Owners who will have responsibility for investigating any breach of information that is within their function.

1.11.4 The management of data security incidents or breaches reported involves containing and recovering any compromised information, assessing the harm or risk posed by the breach, notifying the affected individuals or relevant authorities where necessary and determining mitigation needed to prevent further occurrence of similar incidents. The risk assessment is based on the likely or actual harm to individuals, number of individuals affected and the level of sensitivity of the personal information compromised. In most of the incidents reported the risk level was low as the data compromised was either contained, not sensitive, encrypted or only a few individuals were affected. See Annex C.

1.11.5 In 2016/17, there were 138 information security incidents reported, compared to 102 in the previous financial year. The increase in incidents reported does not necessarily mean that more information was compromised but could be due to the higher level of awareness. Most of the reported incidents were as a result of information disclosed in error or lost or as a result of stolen hardware. A breakdown of the nature of incidents reported is illustrated in Annex C.

1.11.6 Whilst it is not a requirement under the current legislation to report breaches to the ICO, this is recommended where there is a likelihood of significant harm to the individuals or a large number of individuals are affected. Under the GDPR the Council will be required to report breaches to the ICO with 72 hours from the time the Council is made aware of the incident.

1.11.7 Two incidents were reported to the ICO in 2016/17, both have been concluded with no enforcement action due to sufficient remedial measures taken by the Council. This compares to 3 incidents reported to the ICO in 2015/16 about sending Council tax bill emails, Case management documents and Housing benefit invoices to the wrong recipients. However, all cases were closed with no enforcement action. We have considered all recommendations following these investigations and carry out regular process reviews in order to minimise the risk of further breaches occurring.

1.11.8 During their investigations, the ICO considers controls that the organisations have in place to minimise occurrence of similar incidents and if similar incidents by the same organisation have reported to them. Since April 2016, the ICO has issued 3 civil monetary and 2 enforcement notices penalties to local authorities for breaches of the DPA. The Civil monetary penalties given were for the following data protection security breaches:

- Hampshire County Council; £100,000 - documents of over 100 people found in a disused building
- Norfolk County Council; £60,000 - Files with sensitive information about children in a cabinet sent to a second hand shop
- Basildon Borough Council; £150,000 - Sensitive personal information about a family published on Planning Application portal

1.12 **Data Protection Training**

1.12.1 The current DPA mandatory e-learning training was launched on 4 November 2016 and all members of staff with access to computers are expected to complete it on an annual basis. Completion of this training is monitored regularly by the Information Management Strategy Group (IMSG) and shared with the Corporate Leadership Team. Managers in teams where the training has not been completed are reminded to improve uptake of the training.

1.12.2 By the end of the 2016/17 financial year, 2717 employees had completed the DPA e-learning. This figure represents 57% of the Council employees and takes into account those who do not have access to computers as part of their role. Alternative training is being considered for those without access to computers. The Corporate Leadership Team are still working on improving the completion rate of this training.

1.12.3 To support the training, there has been a “Data-Day” event and a communications campaign held to raise Data Protection awareness. Completion of Data Protection training has also now been included in the appraisal document.

2. Options considered and recommended proposal

2.1 It is important that the Council continues to monitor and report on its performance in relation to access to information requests, information security incidents and training completed. This, together with the oversight of elected Members helps to promote high standards of information governance and continuous improvement.

3. Results of consultation undertaken

3.1 None.

4. Timetable for implementing this decision

4.1 None.

5. Comments from Director of Finance and Corporate Services

5.1 Financial implications
There are no financial implications in relation to the recommendations in this report.

5.2 Legal implications
There are no specific legal implications arising out of the recommendations. However, the Council's performance is subject to external scrutiny by the ICO. The monitoring and reporting on the outcomes of ICO complaints represents good practice and promotes good governance and service improvement.

6. Other implications

Any other specific implications

6.1 How will this contribute to achievement of the Council's Plan?

The monitoring and reporting of the Council's performance for responding and handling access to information requests under FOIA and DPA together with all ICO complaints will promote 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?

The reporting and monitoring on the Council's performance and outcomes of ICO complaints will help reduce the risk of the ICO upholding complaints and taking enforcement action against the Council.

6.3 What is the impact on the organisation?

As set out in 6.1

6.4 Equalities / EIA

As set out in 6.1

6.5 Implications for (or impact on) the environment

None

6.6 Implications for partner organisations?

None

Information provided within this report will also be reported to the Corporate Leadership Team and the Directorate Leadership Teams to raise awareness of the issues in an effort to drive improvement in the compliance to legislation and regulations regarding the security and integrity of information handling and processing activities undertaken by the Council.

Report author(s):

Name and job title:
R Kotonya, Senior Information Governance Officer

Directorate:
Place

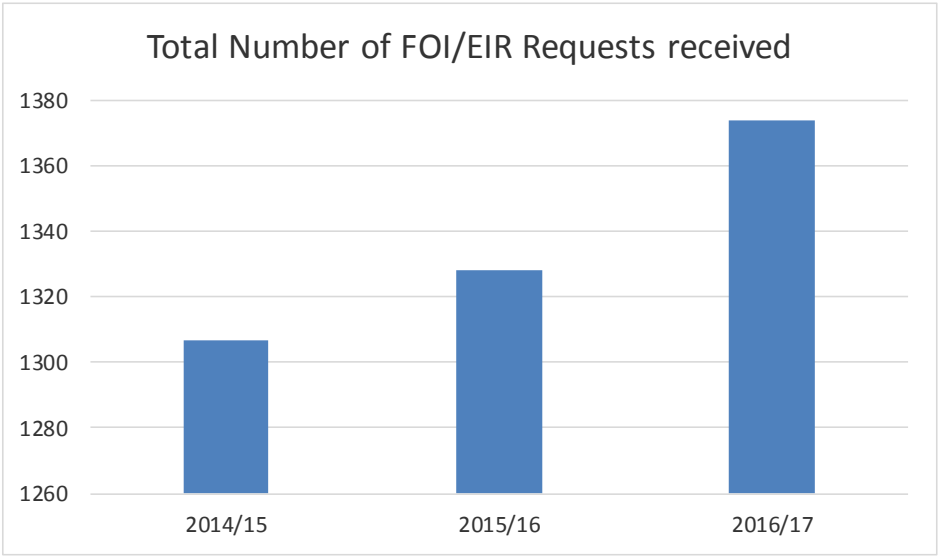
Tel and email contact:
024 7683 2719 Rosebella.kotonya@coventry.gov.uk

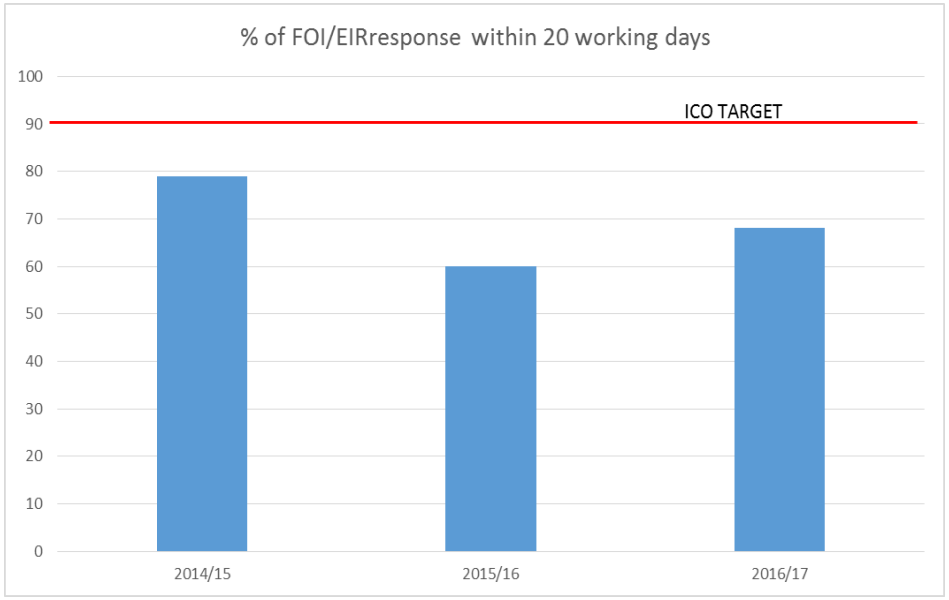
Enquiries should be directed to the above person.

Contributor/approver name	Title	Directorate or organisation	Date doc sent out	Date response received or approved
Contributors:				
Lara Knight	Governance Services Co-ordinator	Place	10/7/17	10/7/17
Sharon Lock	Records Manager	Place	9/6/17	10/7/17
Joe Sansom	Programme Manager – Transformation Project Team	People	26/6/17	29/6/17
Lisa Commane	Director of Customer Services and Transformation	People	26/6/17	6/7/17
Other members				
Names of approvers for submission: (officers and members)				
Finance: Paul Jennings	Finance Manager (Corporate Finance)	Place	11/7/17	11/7/17
Legal: Helen Lynch	Legal Services Manager (Place & Regulatory	Place	11/7/17	11/7/17
Director: Barrie Hastings	Director of Finance and Corporate Services	Place	11/7/17	12/7/17
Members: Cllr George Duggins	Leader- Policy and Leadership		11/7/17	

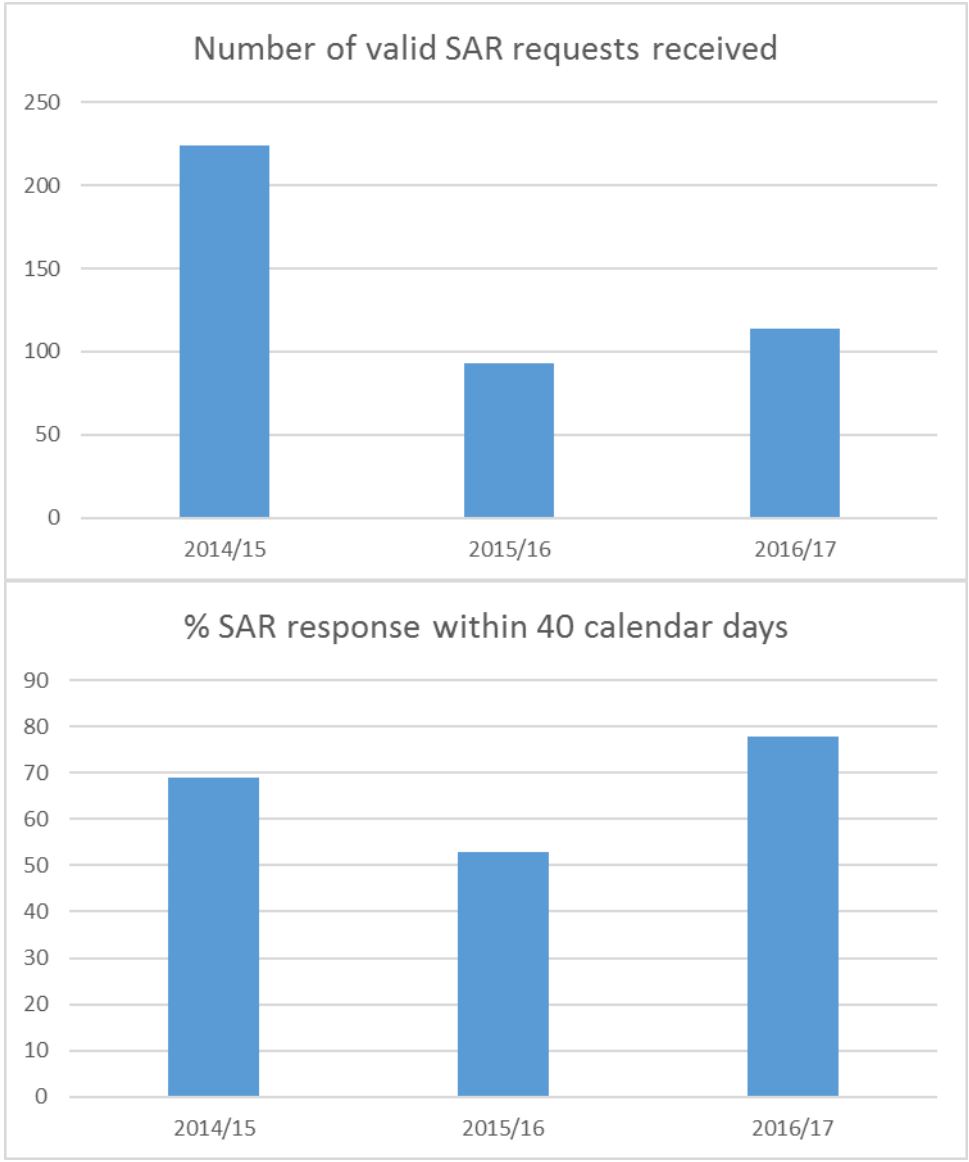
This report is published on the council's website:
www.coventry.gov.uk/councilmeetings

Annex A. Number of FOI/EIR requests received and completion rates in the last 3 years





Annex B. Number of Subject Access Requests (SAR) received and completion rates in the last 3 years



Annex C. Nature of Data protection security breaches reported and severity in 2016/17