Coventry City Council

Public report
Audit and Procurement Committee

Audit and Procurement Committee 15 March 2021

Name of Cabinet Member:
Cabinet Member of Policy and Leadership – Councillor G Duggins

Director Approving Submission of the report:
Director of Law and Governance

Ward(s) affected:
None

Title:
Information Governance Annual Report 2019/2020

Is this a key decision?
No

Executive Summary:

Information is one of the Council's greatest assets and its correct and effective use is a major responsibility and is essential to the successful delivery of the Council's priorities. Ensuring that the Council has effective arrangements in place to manage and protect the information it holds is a priority.

Data protection legislation sets out the requirements on public organisations to manage information assets appropriately and how they should respond to requests for information. The Information Commissioner's Office (ICO) is the UK's independent supervisory authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals, and monitors compliance with legislation.

The Information Governance function supports the Council's compliance with the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations (EIR), General Data Protection Regulations GDPR (now UK GDPR) and Data Protection Act (DPA) 2018. The Council has a statutory obligation to comply with this framework by responding appropriately to requests and managing personal data appropriately.

The Information Governance Team supports the organisation in meeting these requirements, co-ordinating and providing support to the Council's activity including co-ordinating requests received under legislation. The Data Protection Team, comprising the Data Protection Officer (DPO), the Head of Information Governance, and four Information Governance Officers) manage the organisations' approach to data protection including the management of data protection security incidents.

This report provides a summary of the Council's performance during 2019/2020 in responding to requests for information received under the Freedom of Information Act, Environmental Information Regulations and Data Protection Act. It also reports on the management of data protection security incidents reported and data protection training.

Recommendations:

1) The Audit and Procurement Committee is recommended to note:

    a) The Council's performance on Freedom of Information, Subject Access and other Data Protection Act requests, including the outcomes of internal reviews and the number and outcome of complaints made to the ICO.

    b) Reporting and management of data security incidents.

    c) Data Protection training compliance

2) The Audit and Procurement Committee is recommended to identify any comments or recommendations

List of Appendices included:
None

Background papers:
None

Other useful documents
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

Report title: Information Governance Annual Report 2019/20

1. Background

1.1 The Council's Information Governance arrangements support it in managing information and complying with legislation and regulations including the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR), General Data Protection Regulation (now UK GDPR) and Data Protection Act (DPA) 2018. The Council has a statutory obligation to comply with this framework by responding appropriately to requests and managing personal data appropriately.

1.2 The Council is obliged to respond to information requests under the 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 the 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 Information Governance Team as an FOI/EIR internal review.

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

1.4 The DPA 2018 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 and have sufficient information about the request. Following the introduction of the GDPR, the timescale for responding to these requests was reduced from 40 calendar days to one month, starting on the day of receipt. Authorities can extend the time taken to respond by a further two months if the request is complex or a number of requests have been received from the individual, e.g. other types of requests relating to individuals' rights.

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, as 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 Information Governance Team maintains a central log that includes exemptions relied on when personal data is shared with third parties. The Team gives advice and assesses whether the Council is allowed to disclose the information or not.

1.7 The Council also has arrangements in place to manage data protection security incidents where has been or could be compromised and the Council's Data Protection Team records, investigates and where necessary, recommends actions to be taken based on the risk level.

1.8 The Information Governance Team also supports the Council in understanding the impact of plans, projects and activities on data protection through a process of impact assessments to support decision-making. The Council also has arrangements in place to support the sharing of data where appropriate and the team provide support in the preparation and sign off of on-going and one-off data sharing agreements.

1.9 While this report covers the year 2019/20 and a future report will address the current year, the landscape in which public authorities are now operating has changed significantly since 2018, which saw the introduction of the GDPR and the new Data Protection Act 2018 (DPA 2018). At the end of the 2019/20 year, the country went into lockdown as part of its response to the Covid 19 pandemic and the impact of Brexit has subsequently led to introduction of the UK GDPR.

1.10 The pandemic has resulted in significant changes to ways of working and priorities. During this period, the Information Governance Team has supported the Council to adapt and keep working effectively. It has facilitated the rapid turnaround of sharing requests and needs whilst ensuring requests have been properly assessed to confirm that the personal data of the people concerned is used correctly, is properly protected, is only used for the purpose for which it has been provided an only retained as long as is necessary and in keeping individuals informed of how their data is handled. This has allowed data to flow compliantly for the purposes of the Council's pandemic response. It has supported the organisation as new ways of working have been introduced to meet needs while ensuring the continuing protection of information.

1.11 The introduction of GDPR brought an increase in requests for personal data (SARs), it strengthens the rights of individuals and promotes their control over the way that their data is used. The pandemic and subsequent lockdowns have seen little difference in the numbers of requests.

1.12 The Council's approach to information governance continues to evolve and priorities include re-establishing the Information Management Strategy Group following a review of its terms of reference and the appointment of the Director of Law and Governance as the Council's Senior Information Risk Officer; the establishment of an effective framework for the management of information risks; the introduction of a new management system for dealing with information requests; launching a new scheme of data protection and information security training and ensuring comprehensive take up; and ensuring that the Council's activities and allocation of resources continue to support effective information governance arrangements.

1.13 Requests for information

1.13.1 The number of Freedom of Information Requests received by the Council increased year on year to 1,540 in 2018/19 and a small reduction to 1,474 was seen in 2019/20 (see table 1). The Council responded to 78% of FOIA/EIR requests within the target time of 20 working days in 2019/20 compared to 62% for the previous year (see table 2). While the proportion of requests dealt with within the target time has improved, performance remains below the 90% target set by the ICO.

1.13.2 The Council received 48 requests for internal reviews in the year 2019/20. The Council responded to these with the following outcomes:

- 13 were not upheld – the exemptions that had been applied were maintained and no further information was provided
- 11 were not upheld – more information or clarification was provided
- 6 were partially upheld – some further was information provided
- 15 were upheld - information was provided
- 1 was upheld – a further exemption was engaged
- 1 was withdrawn
- 1 was closed with no further action

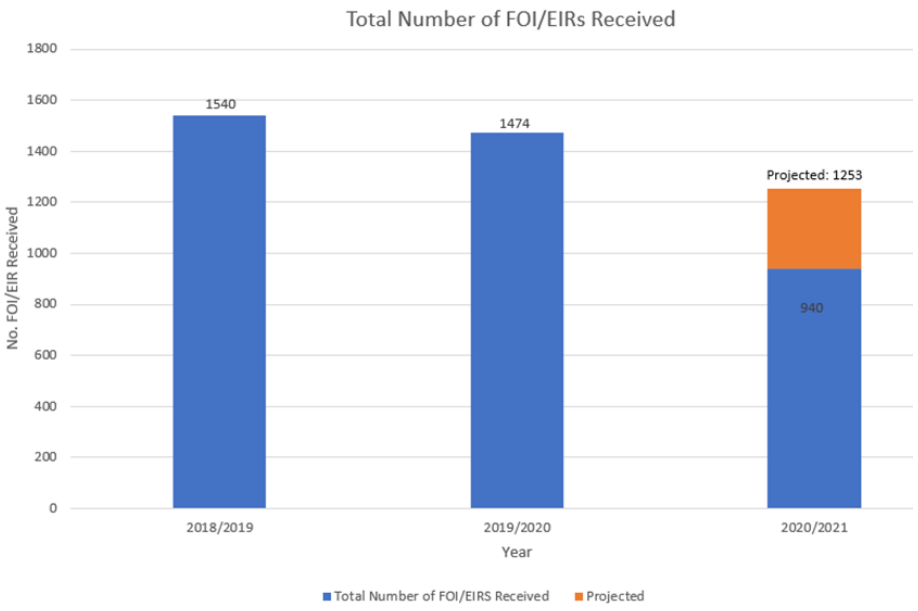
(32 requests for internal reviews have been received during the first three quarters of 2020/21).

1.13.3 Five complaints were referred to the ICO during 2019/20. The reasons and outcomes for these were:

- Requester stated that they had not received a response. The response to the FOI had been issued on day 23. The was ICO notified and there was no further action.
- The response was reviewed and a revised response issued. The ICO was notified and there was no further action.
- The requester submitted an amended request and the complaint was withdrawn.
- A complaint that the requested information had not been provided was not upheld and the ICO found in favour of the City Council.
- In response to a complaint about the handling of an EIR request, the complaint was not upheld and the ICO issued a decision notice.

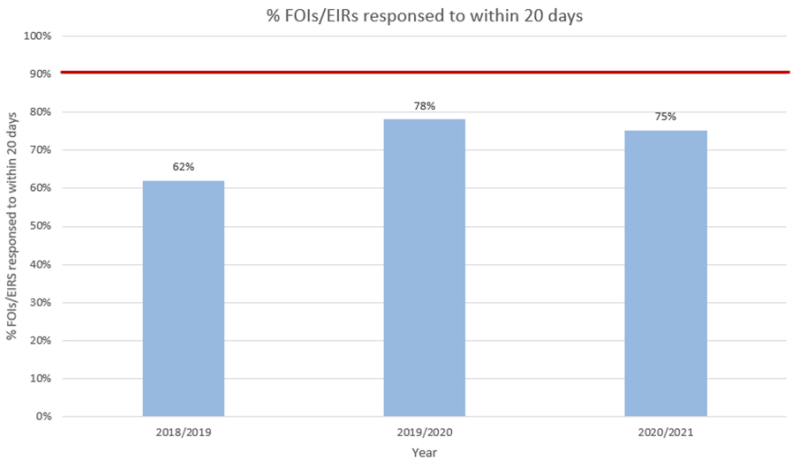
(Two complaints have been referred to the ICO during the first three quarters of 2020/21 and both are awaiting the allocation of an ICO case worker. No details relating to the complaints have been made available).

Table 1. Number of FOI/EIR requests received



Figures for 2020/2021 Financial Year include the data for April-December 2020 (Q1-3)
If current trend continues, expect 1,253 FOI/EIRs to be received in 2020/2021

Table 2. Proportion of FOI/EIR requests completed within target time

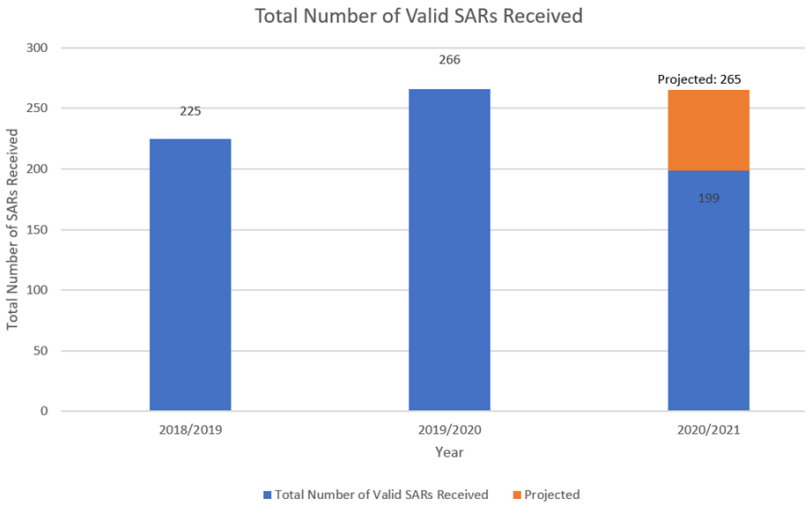


ICO Adequate Response Rate – 90%
Figures for 2020/2021 Financial Year include the data for April-December 2020 (Q1-3)

1.13.4 The City Council already publishes a significant amount of information and identifying opportunities to increase the volume and type of information published (subject to legal compliance) will increase transparency and help to reduce the number of FOI's the Council receives, if the information is already available.

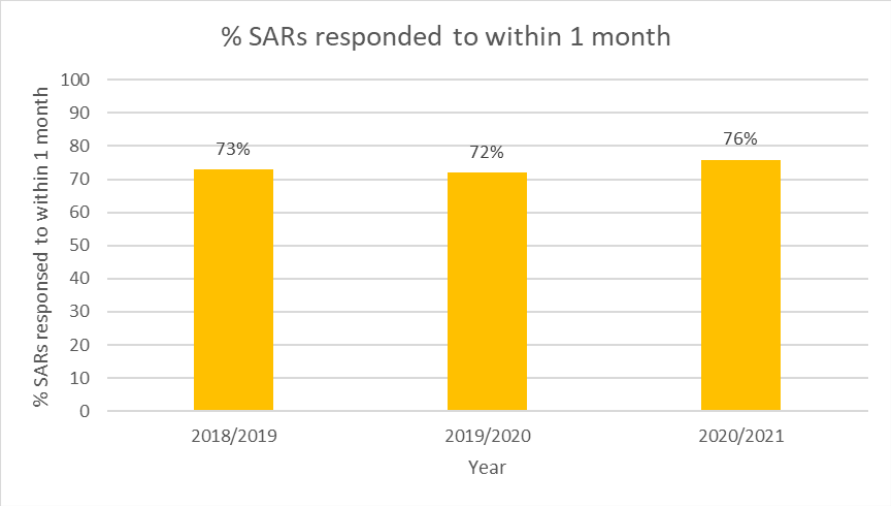
1.13.5 The Council received 266 valid Subject Access Requests (SARs) during the course of 2019/20, compared to 225 in the previous year (see table 3). The number of SARs has been rising year on year with a significant increase seen following the introduction of the GDPR. While the Council receives fewer SARs than other information requests, many of these are complex and can involve managing significant amounts of sensitive information. The introduction of the GDPR also reduced the required response time for responding to SARs from 40 days to one calendar month. The completion rate within the target time has remained broadly the same at 72% (see table 4).

Table 3. Number of SAR's received



Figures for 2020/2021 Financial Year include the data for April-December 2020 (Q1-3)
If current course continues, expect 265 SARs to be received in 2020/2021

Table 4. Proportion of SARs responded to within target time



NB. % complete within either 1 month, or 3 months where complex extension applies in 2020/2021 is 81%
Figures for 2020/2021 Financial Year include the data for April-December 2020 (Q1-3)

1.13.6 The Council received four requests to carry out an internal review into a SAR application during 2019/10. In three cases, further information was provided. The information requested in the fourth was not held by the Council. (13 requests for reviews have been received during the first three quarters of 2020/21).

1.13.7 One complaint was referred to the ICO and the exemption applied by the Council was upheld. (One complaint has been referred to the ICO during the first three quarters of 2020/21.)

1.14 Data Protection Security Incidents and Reports

1.14.1 Protecting information from theft, loss, unauthorised access, abuse and misuse is important in order 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.

1.14.2 An effective data protection security incident reporting process ensures that any breaches are contained and managed promptly and the outcomes of the investigation are used to inform reviews of the controls that are in place to keep personal information secure. The reporting of near misses is also actively encouraged. The process allows the organisation to learn from mistakes and prevent serious personal data breaches that may cause harm to individuals and the Council.

1.14.3 The Council encourages the reporting the reporting of near misses and potential breaches as this promotes awareness, avoids complacency thus reducing the likelihood of a serious breach to information. Increased data protection awareness encourages an increase in reports and investigations although not all reported incidents will have resulted in a breach. Even where there is no breach, incidents can provide valuable insight into training requirements and processes and procedures which may need to be strengthened as a preventative measure.

1.14.5 A risk assessment is used to inform the action required and is based on the likely or actual harm to individuals, number of individuals affected and the level of sensitivity of the personal information compromised. The risk assessment score used is based on guidance issued by the Health and Social Care Information Centre (HSCIC) which takes into account the impact and likelihood the breach would have on the individuals.

1.14.6 In 2019/20, the Data Protection Team received 219 reports of potential data security incidents. Of these, 156 did not involve a breach of personal data. These included for example near misses, loss or theft of equipment, cases where technical measures prevented access to data and incidents where a potential breach was contained. Of the 63 incidents where a breach of personal data was identified, 42 were identified as low risk, 13 low/medium, 7 medium and 1 high. The majority of these were classified as information being disclosed in error with 5 incidents logged as a result of unauthorised access and 4 as technical/ procedural failures. The GDPR introduced requirements for personal data breaches that meet certain thresholds to be reported to the ICO. No self-reports were made to the ICO during 2019/20 compared to one in 2018/19. One complaint was made by a data subject directly to the ICO who advised an informal resolution with the City Council. While there had been a technical/procedural error, no data had been breached.

1.15 Training and Awareness

1.15.1 Data Protection training is key to ensuring staff are aware of their responsibilities. Training is currently delivered through the Council's e-learning platform and annual completion of the data protection course is mandatory for all staff handling personal data. Staff who do not have access to a computer in their role (not office based) and those with minimal personal data involved in their role are provided with alternative training. This ensures that an appropriate level of understanding and awareness is reached that is relevant to their role/responsibilities. In addition to the Data Protection Training there is also a need to provide specific Cyber Security training. Data Protection and Cyber Security are two separate complementary areas with equal importance for different reasons. Data Protection is about how we protect personal data that we collect and process, regardless of format (online/paper) and remain compliant to information laws. Cyber security is how individuals and organisations reduce the risk of cyber-attack, malware, identifying malicious emails. Its focus is on how the devices (smartphones, laptops, tablets and computers) and the services accessed are protected from theft, damage, and unauthorised access to information we store on our devices, and online. As cyber-attacks generally involve targeting unsuspecting people, luring them to either provide information or a way into our systems. Cyber Security awareness will support employees to be more vigilant about their use of ICT and how that can be exploited opportunistically.

1.15.2 For the 2019/20 year, the Council reported a completion rate of the Council's mandatory data protection training of 90.64% when completing NHS Data Security and Protection Toolkit. This self-assessment tool enables public authorities to demonstrate their ability and commitment to maintain the confidentiality and security of personal information, particularly health and social care personal records. The Council met all of the standards, with the exception of that related to training which requires a minimum completion rate of 95%.

1.15.3 Meeting the level of 95% compliance is a priority as it is a key part of the Council's approach to protecting data and provides assurance to other organisations when they share data with the City Council. Work continues to promote take up across the authority and plans are in place for the roll out of new refreshed online training.

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, data protection security incidents and training completed in order to promote best practice information governance and drive continuous improvement in the Council's ability to comply with the laws relating to information.

3 Results of consultation undertaken

3.1 None

4 Timetable for implementing this decision

4.1 None

5 Comments from the Director of Finance and the Director of Law and Governance

5.1 Financial implications

There are no specific financial implications resulting from the issues within this report although it is worth noting that the Information Commissioner's Office is able to levy significant fines for serious non-compliance with the legislation surrounding the management of information.

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, who have the authority to impose sanctions upon the Council for non-compliance. The monitoring and reporting on the outcomes of ICO complaints represents good practice and promotes good governance and service improvement.

6 Other implications

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

The monitoring and reporting of the Council's performance regarding responding to, and handling access to information requests under FOIA and DPA 2018, including any complaints made to the ICO will enable continuous improvement, raise awareness and promote high standards of information governance, fostering a culture of openness and transparency within the Council and demonstrating our commitment to best practice information governance, security, and protection.

6.2 How is risk being managed?

The reporting and monitoring on the Council's performance to information laws 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?

Meeting best practice for information governance will support public confidence in the Council, offering assurance to service users of the council's commitment to data protection and transparency. Partner and client organisations will have the assurance they required in order to engage with the Council and share data. The risks of serious

breaches of personal data/information assets should be reduced thus reducing the likelihood of action by the ICO.

6.4 Equality Impact Assessment (EIA)

The Council's responsibilities under Section 149 of the Equality Act 2010 are supported by UK GDPR/DPA2018, requiring that Special Category Data is afforded extra measures of security to protect that data.

6.5 Implications for (or impact on) climate change and the environment

None

6.6 Implications for partner organisations?

As set out in section 6.3 of the report.

Report authors:
Name and job title:
Sharon Lock, Head of Information Governance

Service:
Law and Governance

Tel and email contact:
Sharon Lock: 024 7697 0982
sharon.lock@coventry.gov.uk

Enquiries should be directed to the above personnel.

Contributor/ approver name	Title	Directorate or organisation	Date doc sent out	Date response received or approved
Contributors:				
Adrian West	Members and Elections Team Manager	Law and Governance	01/03/2021	04/032021
Michelle Salmon	Governance Services Officer	Law and Governance	01/03/2021	01/03/2021
Names of approvers for submission: (officers and members)				
Paul Jennings	Finance Manager (Corporate Finance)	Finance	01/03/2021	01/03/2021
Sarah Harriott	Corporate Governance Lawyer	Law and Governance	01/03/2021	01/03/2021
Julie Newman	Director of Law and Governance	-	01/03/2021	01/03/2021
Councillor G Duggins	Leader and Cabinet Member for Policy and Leadership	-	02/03/2010	

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